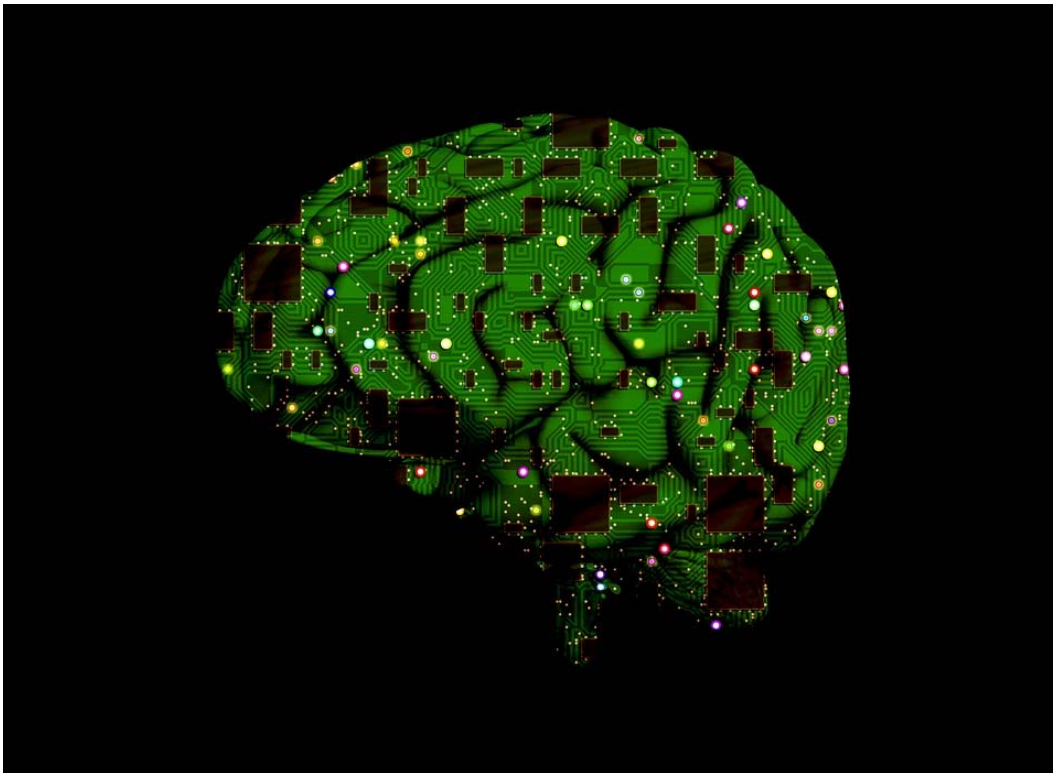
Insights for the Third Offset:

Addressing Challenges of Autonomy and Artificial Intelligence in Military Operations

Larry Lewis

September 2017



This document contains the best opinion of CNA at the time of issue.

It does not necessarily represent the opinion of the sponsor.

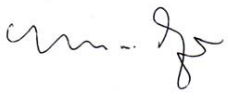
Distribution

DISTRIBUTION STATEMENT A. Approved for Public Release.

Request additional copies of this document through inquiries@cna.org.

Photography Credit: "Processing Artificial Brain Intelligence Circuit," FreeGreatPictures.com.

Approved by: **September 2017**



Mark Geis
Executive Vice President
Center for Naval Analysis

This work was performed under Federal Government Contract No. N00014-16-D-5003.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
09-2017	Final	

4. TITLE AND SUBTITLE
(U) Insights for the Third Offset: Addressing Challenges of Autonomy and Artificial Intelligence in Military Operations

5a. CONTRACT NUMBER
N00014-16-D-5003

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
0605154N

6. AUTHOR(S)
Larry Lewis

5d. PROJECT NUMBER
R0148

5e. TASK NUMBER
D180.00

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Center for Naval Analyses
3003 Washington Blvd
Arlington, VA 22201

8. PERFORMING ORGANIZATION REPORT NUMBER
DRM-2017-U-016281-Final

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of the Chief of Naval Operations
(OPNAV N81)
Navy Department Pentagon
Washington, DC 20350

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A. Approved for public release.

13. SUPPLEMENTARY NOTES

14. ABSTRACT CNA conducts analysis for the U.S. Navy, the Department of Defense (DOD), and other sponsors, ranging across policy, strategy, organizational processes, technical performance of military systems, and current operations. Because of the expected impact of autonomy and artificial intelligence (AI) to the character of warfare, CNA has created a Center for Autonomy and Artificial Intelligence to focus on these emerging technologies and their significant role in U.S. defense policy and all the military services. The Center combines CNA's strengths and experience in conducting objective analysis of U.S. military operations with focused expertise in autonomy and other aspects of AI. This report, the first created by the new Center, takes lessons and insights from CNA's body of work for the Navy and the joint force, including CNA's field program of embedded analysts in military commands around the world. Though much of the emerging technology examined in this report is new, the approach of applying lessons from U.S. operations and institutional processes to key challenges in leveraging autonomy and AI continues CNA'S applied research paradigm of exploring many opportunities to resolve or work around challenges that have been seen before. The aim of this report is to anticipate challenges of "Third Offset" implementation based on past lessons, and then provide concrete recommendations for promoting the effective incorporation of autonomy, AI, and related technologies in U.S. military operations.

15. SUBJECT TERMS
Autonomy, Artificial Intelligence, AI, Third Offset, Strategy, Deterrence, Interoperability, Fratricide, Civilian Casualties, Coalitions, LOAC, Acquisition, Unmanned, UAS, UxS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Knowledge Center/Robert Richards
U	U	U	SAR	84	**19b. TELEPHONE NUMBER** *(include area code)* 703-824-2123

Abstract

CNA conducts analysis for the U.S. Navy, the Department of Defense (DOD), and other sponsors, ranging across policy, strategy, organizational processes, technical performance of military systems, and current operations. Because of the expected impact of autonomy and artificial intelligence (AI) to the character of warfare, CNA has created a Center for Autonomy and Artificial Intelligence to focus on these emerging technologies and their significant role in U.S. defense policy and all the military services. The Center combines CNA's strengths and experience in conducting objective analysis of U.S. military operations with focused expertise in autonomy and other aspects of AI. This report, the first created by the new Center, takes lessons and insights from CNA's body of work for the Navy and the joint force, including CNA's field program of embedded analysts in military commands around the world. Though much of the emerging technology examined in this report is new, the approach of applying lessons from U.S. operations and institutional processes to key challenges in leveraging autonomy and AI continues CNA'S applied research paradigm of exploring many opportunities to resolve or work around challenges that have been seen before. The aim of this report is to anticipate challenges of "Third Offset" implementation based on past lessons, and then provide concrete recommendations for promoting the effective incorporation of autonomy, AI, and related technologies in U.S. military operations. This report discusses making autonomy and AI militarily effective from an acquisition and technology perspective, and how to pursue these capabilities in ways that are consistent with long-standing U.S. values and that promote broader U.S. national interests.

This page intentionally left blank.

Executive Summary

Throughout history, the ability to adapt technological advances to warfighting has led to fundamental changes in the character of war and the tools used in its conduct. Examples include the development of the crossbow; gunpowder-powered projectile weapons; chemical weapons in World War I; rockets, jet aircraft, and nuclear warheads in World War II; and stealth, unmanned vehicles, and precision-guided munitions in recent decades. Military operations are poised for a revolutionary change with the rapid and advancing progress in artificial intelligence, including the attribute of autonomy. Dominated by the commercial industry and its innovations, the past two years have seen dramatic advances in which machines have been able to complete complex tasks and match or exceed human performance. This trend is expected to continue.

At the same time, key technologies behind the military edge of the United States have proliferated to other pacing competitors, which now have capabilities comparable to those of the U.S. and have developed ways to counter traditional U.S. military strengths. The U.S. response to this new security environment is the "Third Offset" strategy, an asymmetric approach that aims to "exploit all the advances in artificial intelligence and autonomy … to achieve a step increase in performance that the department [U.S. Department of Defense] believes will strengthen conventional deterrence."[1]

Unlike past offset strategies, this approach must reflect the new reality that for the underlying technology, commercial research and development (R&D) efforts will dwarf that of the U.S. military. Thus the Third Offset must rely on developments in the commercial sector as well as DOD's R&D programs. Of course, commercial development will be equally exploitable by many states—and by non-state actors for that matter—so the ability to quickly identify developments and integrate them into fielded systems will be critical in this new, rapidly evolving technological environment. This creates challenges for a U.S. military characterized by a slow and deliberate acquisition process. In addition, the U.S. military has struggled to

[1] Cheryl Pellerin, "Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence," DOD News, October 31, 2016, https://www.defense.gov/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence.

integrate technologically advanced systems to date, plagued by significant and persistent interoperability challenges that both reduce effectiveness and increase the risk of fratricide and civilian casualties. These interoperability challenges could be even more significant for autonomous systems.

At the same time, the most controversial aspect of this new technology—should weapon systems operating autonomously (without a human operator) be allowed to use lethal force—could have significant impact on the ability and will of the U.S. to field and use such systems. About a dozen states and some nongovernmental organizations (NGOs), along with some prominent scientists, have been vocal about a preemptive ban on such weapons, citing concerns about civilian casualties, the difficulties of machines complying with international humanitarian law (IHL), and other ethical considerations. Likewise, U.S. operators and senior leaders will need to decide that these systems are reliable and can be trusted on the battlefield. And our allies are already expressing some concerns regarding the use of these new technologies in war, which could strongly impact current and future coalition operations. These are all audiences the U.S. will need to consider, at the same time that other states are moving rapidly toward the use of autonomous systems and the militarization of artificial intelligence overall.

This report examines each area of concern, based on CNA's experience in conducting objective analysis of U.S. military operations, as well as its expertise in autonomy and other aspects of AI. Though much of the emerging technology is new, the approach of applying lessons from U.S. operations and institutional processes to key challenges in leveraging autonomy and AI continues CNA'S applied research paradigm of exploring many opportunities to resolve or work around challenges that have been seen before. The report concludes with concrete recommendations for better leveraging these technologies in support of the Third Offset strategy. It also discusses how this effort does not have to sacrifice U.S. principles and values for military effectiveness. Both goals are possible: making autonomy and AI militarily effective from an acquisition and operational perspective, and pursuing these capabilities in ways that are consistent with longstanding U.S. principles in the advancement of broader U.S. national interests.

Many advances, some unforeseeable, are expected in the coming decades because of technological advances involving autonomy and AI. At the same time, there are actions the U.S. can take now to best prepare for these advancements and leverage them effectively. This report details four deliberate efforts needed in the near term to overcome key challenges in leveraging autonomy and AI in the Third Offset. Those efforts are:

- Becoming a fast follower to rapidly develop capabilities leveraging key technologies

- Prioritizing interoperability of autonomous systems to improve their effectiveness
- Taking specific actions to help autonomous weapon systems avoid mishaps such as friendly fire and civilian casualties
- Promoting freedom of action for the use of autonomy and AI in operations with multiple audiences

Recommended actions for each of these efforts are summarized below:

Aim to be an effective fast follower of autonomous and artificial intelligence technologies. This includes the following actions:

- **Build DOD technical expertise.** Cultivate technical expertise on autonomy and AI in the military services capable of identifying specific technical requirements needed for achieving military capabilities.
- **Prioritize military R&D resources,** leveraging a fast-follower approach. Instead of trying to cover all aspects of autonomy and AI, prioritize R&D resources to areas of the highest importance, or to areas not receiving attention in the commercial sector.
- **Monitor and integrate specific commercial developments.** DOD technical expertise should track targeted autonomy and AI developments in the commercial sector, looking for ways to rapidly integrate those developments into military systems.
- **Track developments by others.** Track technological developments towards militarization of autonomy and artificial intelligence by key states and non-state actors, leveraging them for evaluation of U.S. operational plans, needed U.S. capabilities, and possible ways the U.S. can learn from these other efforts.
- **Introduce a learning loop.** Conduct in-stride learning efforts for existing DOD innovation initiatives (e.g., Project Maven) in order to make efforts meeting urgent operational needs through autonomy and AI more effective.

Prioritize interoperability of autonomous systems. This includes:

- **Include a programmatic focus on interoperability.** Given the greater vulnerability autonomous systems can have to interoperability challenges, especially for those using lethal force, program offices give close attention to interoperability for autonomous systems as discussed in this report.

- **Policy requirement for interoperability.** Make a requirement for observing interoperability best practices as part of the senior review of fully autonomous systems required in DODD 3000.09.

- **Reduce risk through live events.** Use regularly scheduled risk-reduction live events (such as exercises) throughout the development life-cycle of autonomous systems to reduce risk.

- **Marry experimentation with data and analysis.** Include data collection and analysis during experimentation events in order to supplement and confirm operator and observer impressions, and accelerate the process for improving capabilities overall.

Take specific measures to help lethal autonomous systems avoid inadvertent engagements, including:

- **Monitor for misidentifications.** Autonomous systems should give careful attention to the possibility of misidentification, including cross-checks of different kinds of identifying information and flagging potential conflicts or inconsistencies—for example, identifying that an entity has kinematics that are inconsistent with a suspected platform or target type.

- **Include robust IFF measures.** Sensors for autonomous systems should ensure compatibility with appropriate anti–friendly fire measures.

- **Leverage available information.** Autonomous does not necessarily mean isolated. In light of mission requirements, autonomous systems should be provided with information and intelligence when possible to ensure current situational awareness and inform optimal engagement decisions.

- **Consider civilian casualties.** Autonomous systems should give careful consideration and make every precaution to avoid civilian casualties, including specific measures described in this report.

- **Develop DODD 3000.09 senior review criteria.** These considerations should be made part of the required senior-level review for development and fielding of autonomous systems per DODD 3000.09.

Take steps to be able to employ autonomy and AI in operations if necessary to deter and defend itself against critical threats:

- **Examine other risks of lethal autonomy.** This report examines the risk of inadvertent engagements by lethal autonomous weapon systems. A further study should examine a number of other potential risks presented by lethal autonomy that are humanitarian, ethical, and strategic in nature.

- **Familiarization training.** Provide extensive familiarization training for operators and operational commanders regarding systems with autonomy and artificial intelligence, preferably over a wide range of scenarios and missions.

- **New approach to Test and Evaluation.** To ensure reliability and confidence in non-deterministic systems, develop a new approach to Test and Evaluation processes for systems employing autonomy and AI, including specific features described in this report.

- **Export policy for autonomy.** The U.S. government should develop a U.S. export policy and accompanying review process to address the risks of U.S. technology being used in lethal autonomy by others.

- **Identify and address coalition friction points.** Work with allies to resolve policy and interoperability issues associated with the operational use of autonomy and AI. Start with key allies such as the UK, Australia, and Canada.

- **Substantive engagements,** with Congress, in international venues, and with civil society groups. Continue meaningful involvement with Congress, in international forums regarding autonomy and AI in military operations, and other important audiences.

- **Learn from the Second Offset.** The U.S. military should learn from the success of the Second Offset and include both precision and promoting humanitarian goals such as sparing civilians in war in its implementation of and communications regarding the Third Offset.

This page intentionally left blank.

Contents

Glossary

ACDA	Arms Control and Disarmament Agency
AI	Artificial intelligence
AoA	Analysis of Alternatives
ASCIET	All Service Combat Identification Evaluation Team
ATACMS	Army Tactical Missile System
AWCFT	Algorithmic Warfare Cross-Functional Team
BFT	Blue Force Tracker
CCW	Convention for Certain Conventional Weapons
CENTCOM	U.S. Central Command
CONOPS	Concept of operations
COTS	Commercial off-the-shelf
CWC	Chemical Weapons Convention
DEP	Distributed Engineering Plant
DIUx	Defense Innovation Unit Experimental
DODD	DOD Directive
DSB	Defense Science Board
FLOT	Forward Line of Own Troops
GGE	Group of Government Experts
GPS	Global Positioning System
ICRC	International Committee of the Red Cross
IED	Improvised explosive device
IFF	Identification Friend or Foe
IHL	International humanitarian law
IOC	Initial Operational Capability
IR	Infrared
ISR	Intelligence, surveillance, and reconnaissance
JADO-JEZ	Joint Air Defense Operation–Joint Engagement Zone
JCIET	Joint Combat Identification Evaluation Team

JFCOM	U.S. Joint Forces Command
LOAC	Law of Armed Conflict
NATO	North Atlantic Treaty Organization
NDAA	National Defense Authorization Act
NGO	Nongovernmental organization
OSD	Office of the Secretary of Defense
PED	Processing, exploitation, and dissemination
PPG	Presidential Policy Guidance
PPLI	Precise Participant Location Information
R&D	Research and development
ROE	Rules of engagement
SCO	Strategic Capabilities Office
SOF	Special Operations Forces
T&E	Test and Evaluation
TTP	Tactics, techniques, and procedures
UONS	Urgent Operational Needs System
WMD	Weapons of mass destruction

Introduction

Throughout history, the ability to adapt technological advances to warfighting has led to fundamental changes in how war is conducted and the tools used in its conduct. Examples include the development of the crossbow; gunpowder-powered projectile weapons; chemical weapons in World War I; rockets, jet aircraft, and nuclear warheads in World War II; and stealth, unmanned vehicles, and precision-guided munitions in recent decades. Modern militaries recognize this value of technology and constantly examine how it can be most effectively used in warfare.

The past few years have seen exponential progress in artificial intelligence (AI), defined as "the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings."[2] This progress has been dominated by commercial industry and its constant innovations. The past two years have seen dramatic advances in which machines have been able to complete complex tasks and match or exceed human performance. Just a short list of some of these advances includes:

- AI defeated the reigning world champion in Go, a game so much more "complex" than chess that, prior to this event, most AI experts believed that it could not be done for another 15–20 years
- AI predicted the immediate future (by generating a short video clip) by examining a single photograph (and is also able to predict the future from studying video frames)
- AI automatically inferred the rules that govern the behavior of individual robots within a robotic swarm simply by watching
- An AI communication system invented its own encryption scheme, without being taught specific cryptographic algorithms (and without revealing its method to researchers).

[2] Encyclopedia Britannica, s.v. "artificial intelligence," https://www.britannica.com/technology/artificial-intelligence.

- An AI translation algorithm invented its own "interlingua" language to more effectively translate between any two languages (without being taught to do so by humans)

- An AI-based medical diagnosis system at the Houston Methodist Research Institute in Texas achieved 99 percent accuracy in reviewing millions of mammograms (at a rate 30 times faster than humans).[3]

These advances in AI raise profound questions for humanity to wrestle with, such as what roles we allow machines to play, what decisions we allow them to make, and what values we should instill in them. This development will have a radical influence in all areas of life, and is expected to have a revolutionary impact on military operations, on par with the invention of gunpowder and nuclear weapons.

It is no surprise then that the advances in artificial intelligence, including the promising attribute of autonomy, are of significant interest to states and their militaries around the world. The United States has identified leveraging artificial intelligence and the capability of autonomy as key elements of a new national military strategy: the "Third Offset." The U.S. views its ability to effectively leverage this technology as critical to the success of this offset in order to keep a military edge over potential adversaries and provide an effective deterrent to major conflict. But this success is not guaranteed—the U.S. faces considerable challenges in meeting this goal. For example, a U.S. military advantage in this area will be contested by other States, illustrated in Russian President Vladimir Putin's recent remark that "the one who becomes the leader in this sphere [artificial intelligence] will be the ruler of the world."[4] The set of challenges inherent in the Third Offset strategy is best understood by first considering the purpose of offset strategies and what strategies the U.S. has adopted in the past.

Background: what is an offset strategy?

The essence of an offset strategy is illustrated in the story of David and Goliath. This is an example of unequally matched combatants where the odds seem heavily in favor of the giant Philistine warrior, Goliath, over the Israelite boy shepherd, David. In the story, even Goliath himself considers his competitor unequal to the task, but in the end it is David who prevails by using a different approach, capitalizing on a noncombat skill and hurling a stone from a sling.

[3] List taken from Andrew Ilachinski, *AI, Robots, and Swarms: Issues, Questions, and Recommended Studies,* CNA Research Memorandum DRM-2017-U-014796-Final, January 2017.

[4] "Putin: Leader in Artificial Intelligence Will Rule the World," Associated Press, September 1, 2017.

This story may be the first documented use of an offset strategy. An offset strategy has been described as: "Rather than match an opponent in an unfavorable competition, changing the competition to more favorable footing enables the application of strengths to a problem that is otherwise either unwinnable or winnable only at unacceptable cost."[5] The U.S. has at various times found itself in the position of being unable to counter a potential threat head on, and instead found asymmetric solutions to deter and thus counter the threat. Since World War II, the U.S. has announced three such offset strategies: the first near the tail end of the Korean War, the second in the 1970s, and the third in 2014. Each is summarized in turn.

First offset: nuclear deterrence to conventional capabilities

The First Offset strategy came about at the start of the Eisenhower administration, in the backdrop of a stalemated Korean war, which the U.S. saw as one example of many where the Soviet Union was promoting regional instability to counter U.S. hegemony. U.S. military might seemed outmatched as Soviet conventional military ground forces dwarfed those of the U.S: 175 active divisions and another 125 reserve divisions in the Soviet military versus only 29 active and 7 reserve divisions in the U.S. Army and Marines. It was not considered feasible to build up U.S. ground forces to Soviet levels, especially given fiscal constraints at the time. Thus U.S. efforts to try and contain Soviet expansion with conventional forces seemed doomed.[6]

At the same time, the U.S. had a clear lead in its growing nuclear stockpile after World War II. The Eisenhower administration saw in this an opportunity to solve its problem: reliance on its nuclear capabilities to counter greater Soviet conventional strength. This idea became the First Offset, then entitled the "New Look" defense policy, issued in October 1953. Under this policy, the U.S. would contain the threat of Soviet expansion by the threat of using nuclear weapons in response. This approach was seen to provide "a maximum deterrent at a bearable cost."[7]

This Offset Strategy had two primary components: nuclear devices and delivery capability. The United States had, and maintained, superiority in both of these components. At the end of 1952, the U.S. had 841 nuclear warheads, compared to the Soviets, who were estimated to have 120. Furthermore, the U.S. was growing its stockpile at a rate twice that of the Soviets. And the U.S. had recently demonstrated

[5] Wikipedia, "Offset Strategy," last modified January 21, 2017, accessed April 2, 2017, https://en.wikipedia.org/wiki/Offset_strategy.

[6] Peter Grier, "The First Offset," *Air Force Magazine,* June 2016.

[7] Ibid.

its first thermonuclear device, the hydrogen bomb, with a destructive yield many times that of a fission device. For nuclear weapon delivery, the U.S. had the jet-propulsion B-47 bomber and was developing the B-52, entering active service in 1955. (Soviet bombers were slower, propeller-driven aircraft.) The U.S. also had a strategic advantage in basing, able to use allied bases in NATO Europe and Asia. The Soviets lacked these alliances, and so did not have air bases close to U.S. territory.[8]

Growing concerns about this deterrent approach stemmed from the apparent lack of U.S. resolve to actually use nuclear weapons in response to many possible scenarios. Allies began to wonder if they could count on U.S. support in response to Soviet actions. Gradually, the Soviet Union reached relative parity with the U.S. in nuclear capabilities, and by the 1970s it had developed a second-strike capability that resulted in the doctrine of "mutually assured destruction."[9] In this dangerously destabilized environment, the U.S. began searching for another form of deterrence.

Second offset: reconnaissance and precision strike

In the 1970s, U.S. defense officials were faced with the potential threat of a Soviet conventional-force invasion of central Europe.[10] Soviet forces had a great numerical advantage, up to three times what U.S. and NATO forces had available in terms of personnel and armored vehicles. The U.S. and its allies were unable to muster sufficient numbers to counter the strength of the Soviet force directly. The U.S. saw advancements in microelectronics and computers as an opportunity to create another form of offset: improving conventional capabilities and creating an asymmetric advantage to counter their numerical edge.[11] This advantage consisted of using advanced technology to enable better information on the battlefield and develop the ability to conduct precision strikes in order to improve combat effectiveness.

[8] Ibid.

[9] Van Jackson, "Superiority at Any Price? Political Consequences of the First Offset Strategy," War on the Rocks, October 30 2014, https://warontherocks.com/2014/10/superiority-at-any-price-political-consequences-of-the-first-offset-strategy/; ibid.

[10] Robert Tomeo, "Why the Cold War Offset Strategy Was All about Deterrence and Stealth," War on the Rocks, January 14, 2015, https://warontherocks.com/2015/01/why-the-cold-war-offset-strategy-was-all-about-deterrence-and-stealth/.

[11] Secretary of Defense Chuck Hagel, keynote speech delivered at Reagan National Defense Forum, Ronald Reagan Presidential Library, November 15, 2014, https://www.defense.gov/News/Speeches/Speech-View/Article/606635/.

The Second Offset was not a broad effort to generally improve all weapon systems through better technology. Rather, it identified specific enabling capabilities for particular operational requirements and pursued their development over the course of decades. In 1991, Operation Desert Storm displayed the results of the Second Offset efforts. Desert Storm was seen as a sweeping success, and touted as the new American way of war.[12] In particular, there were three advanced technology components of the Second Offset that contributed to Desert Storm's success: reconnaissance, situational awareness, and integrated action; suppression of enemy defenses; and precision-guided munitions. Collectively, these capabilities—and a well-led, well-trained force using them—resulted in a decisive victory marked with a rapid end, minimal Coalition casualties, and sharply reduced civilian casualties compared to previous armed conflicts.[13]

Third offset: operationalizing AI and autonomy

This U.S. capability to conduct a new way of war was again put on display in operations in Afghanistan in 2001 and in Iraq in 2003. Again, major combat operations were rapid and decisive. However, both of these operations transitioned into extended counterinsurgency and stability operations that expended significant U.S. military resources and attention for the next 15 years.[14] Meanwhile, key enabling capabilities of the Second Offset—such as network-based warfare, precision-guided munitions, advanced missiles, and sophisticated surveillance platforms—have proliferated to other near-peer states. Several countries are causing particular concern: "The pacing competitors—not adversaries—are Russia and China, because they're developing advanced capabilities that potentially worry us." These countries have both capabilities that are comparable with those of the U.S.—for example, digital networks for warfare—and they have also introduced ways to counter U.S. strengths, such as jamming our own networks and disrupting GPS satellites, which are highly relied on by U.S. military systems.[15]

[12] Max Boot, "The New American Way of War," *New York Times,* July 25, 2003, http://www.nytimes.com/cfr/international/20030724faessayv82n4_boot.html?pagewanted=print&position.

[13] William Perry, "Desert Storm and Deterrence," *Foreign Affairs,* Fall 1991, https://www.foreignaffairs.com/articles/iraq/1991-09-01/desert-storm-and-deterrence.

[14] Hagel, keynote speech.

[15] Cheryl Pellerin, "Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence," DOD News, October 31, 2016, https://www.defense.gov/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence.

The initial focus of the Third Offset is to "exploit all the advances in artificial intelligence and autonomy and insert them into DOD's battle networks to achieve a step increase in performance that the department believes will strengthen conventional deterrence."[16]

Unlike past offset strategies, this approach must reflect the new reality: regarding the underlying technology, commercial R&D efforts are going to be much greater than that of DOD. Thus the Third Offset must rely on developments in the commercial sector as well as DOD R&D. Of course, commercial development will be equally exploitable by many states—and nonstate actors—so the ability to quickly identify developments and integrate them into fielded systems will be critical in this new, rapidly evolving technological environment.

At the same time, the U.S. military has been wrestling with national and international policy regarding perhaps the most controversial aspect of the new technology: should weapon systems operating autonomously—without a human operator—be allowed to use lethal force? While the U.S. government has stated that it is pursuing a careful approach to the use of this technology, demonstrated in part by a DOD Directive on lethal autonomy (requiring senior leader approvals for such systems), about a dozen states and some nongovernmental organizations (NGOs) and prominent scientists have been vocal about a preemptive ban on such weapons.[17] Those calling for a ban typically cite concerns about civilian casualties, the difficulties of machines complying with international humanitarian law (IHL), and other normative and ethical considerations. Meanwhile, on the other end of the spectrum, the U.S. is concerned that other states are moving rapidly toward the militarization of artificial intelligence and autonomy.[18]

As DOD begins its implementation of the Third Offset, the U.S. faces a number of potential challenges in its effort to incorporate autonomy and AI into military capabilities as an effective deterrent:

- A near-peer threat gains a military edge over the U.S. by being faster to field military capabilities incorporating state-of-the art commercial technology with autonomy or AI

- The U.S. limits its use of autonomy after interoperability challenges—a particular vulnerability in autonomous weapon systems make autonomous systems less effective than legacy capabilities

[16] Ibid.

[17] DOD Directive 3000.09, *Autonomy in Weapons Systems,* November 21, 2012.

[18] Pellerin, "Third Offset Strategy Bolsters America's Military Deterrence."

- The U.S. limits its use of lethal autonomy after recurring problems with fratricide, civilian casualties, or other inadvertent engagements
- The U.S. finds itself lacking freedom of action to use autonomy because
    - U.S. military operators don't trust and refuse to use autonomous systems, or commanders and political leaders are unwilling to accept the risk
    - Lethal autonomous weapon systems are preemptively banned by international convention
    - Our allies refuse to participate in a coalition or provide intelligence to the U.S. if it uses autonomous weapon platforms in military operations.

All of these potential scenarios are feasible. If any were to occur, it would reduce the deterrent effect that autonomy and artificial intelligence can provide under the Third Offset, and marginalize the potential utility these capabilities could provide to military operations overall. However, they are also avoidable; there is still time for the U.S. to take steps to address each of these real concerns. This report examines each concern and provides recommendations for actions to address them. The pursuit of autonomy and AI in military systems does not have to be done in a way that sacrifices U.S. principles and values for military effectiveness. This report discusses both aspects of this apparent dilemma: making autonomy and AI militarily effective from an acquisition and technology perspective, and how to pursue these capabilities in ways that are consistent with long-standing U.S. values and that promote broader U.S. national interests.

Approach and report topics

CNA conducts analysis for the Navy, DOD, and other sponsors, ranging across policy, strategy, organizational processes, technical performance of military systems, and current operations. Because of the expected impact of autonomous systems and artificial intelligence to the character of warfare, CNA has created a Center for Autonomy and Artificial Intelligence to focus on these emerging technologies and their part in the U.S. military. The Center combines CNA's strengths and experience in conducting objective analysis of U.S. military operations with focused expertise in

autonomy and AI.[19] This report, the first created by the new Center, takes lessons and insights from CNA's body of work for the Navy and the Joint Force, including from its field program of embedded analysts in military commands around the world. Though much of the emerging technology is new, this approach of taking lessons from U.S. operations and institutional processes and applying them to key challenges in leveraging autonomy and AI acknowledges that there are still many opportunities to avoid challenges that have been encountered over the past few years. The aim of this report is to anticipate challenges of Third Offset implementation based on past lessons, and then provide concrete recommendations for promoting the effective incorporation of autonomy, AI, and related technologies in U.S. military operations.

The four chapters reflect potential challenges to the U.S. implementation of the Third Offset strategy:

- **Section 1: Improving acquisition for autonomy and AI.** DOD faces a new environment where commercial R&D of key technology is sizable and rapid; at the same time, DOD's military edge is increasingly threatened by near-peer competitors. This is a challenge for an institution that takes a slow and deliberate approach to acquisition. DOD's ability to take risks and adapt is critical for retaining a military edge in this new environment.

- **Section 2: Promoting interoperability in autonomous systems.** Despite significant advances in network-enabled capabilities, interoperability challenges continue to reduce the effectiveness of current U.S. military systems. Autonomous systems may be even more vulnerable to this challenge. Lessons from past U.S. military operations are essential to overcome interoperability challenges and promote the effectiveness of autonomous systems.

- **Section 3: Mitigating risk in lethal autonomy.** Many concerns have been voiced about "killer robots," and DOD policy includes steps to start addressing the potential risks of lethal autonomy. Real-world operations provide key lessons that lethal autonomous systems—and the U.S. military's senior review process—can heed.

- **Section 4: Addressing concerns about militarization of autonomy.** Concerns over the militarization of this technology can influence its use, thereby limiting its effectiveness as a deterrent. These concerns include trust by operators and leaders, allied support to Coalition operations, international legal and normative frameworks, and media and NGO portrayals. Addressing

[19] For an example of the latter, see Ilachinski, *Robots, AI, and Swarms.*

these concerns effectively can preserve U.S. freedom of action and promote its legitimacy and national interestsThis report is a good start in the exploration of these issues, providing analytic approaches to each topic and specific recommendations for actions that can be taken to address them. Each of these topics is worthy of further study. Hence, this report represents an initial exploration of these topics. Subsequent work at CNA's Center for Autonomy and AI will examine these topics in more depth and explore additional challenges. The conclusions section will also discuss other areas where additional study is needed.

Improving acquisition for autonomy and AI

DOD leadership has emphasized that with the pace of commercial development and aggressive efforts by near-peer adversaries, the U.S. military is in a competition for time. In this environment, maintaining a technological edge necessitates rapid development and fielding of advanced military systems. A key problem in this competition is that DOD acquisition is slow. A previous CNA study on autonomy points out that the average length of an acquisition program is 91 months (7.6 years), as measured from the initiation of an analysis of alternatives (AoA) study to fielding an initial operational capability (IOC). One would think that information technology programs have a much more rapid turnaround, considering the fast and accelerating pace of technology innovation in the commercial sector, but these programs are only slightly shorter in length on average—around 81 months.[20]

This slow pace is often intentional, consistent with the fact that DOD is one of the largest organizations in the world, and is faced with missions involving delivery of lethal force in the most challenging of environments. In light of this, the acquisition process is structured to ensure high quality to meet demanding internal requirements for major equipment often intended to last many decades. That process is designed to promote fiscal accountability per congressionally mandated statutory requirements that support budgetary and oversight functions in both DOD and Congress.[21]

This process, with increasing levels of Congressional and DOD requirements, was less problematic when the U.S. sought to maintain a military edge against the Soviet Union, a largely predictable and steady adversary in terms of advances in military technology. However, it is increasingly incompatible with the current environment. Technology R&D is now driven by the commercial sector, characterized by fast development-to-fielding cycles and often easy to adapt for military applications. The

[20] Ibid.

[21] The standard acquisition process is described in more detail in: Julianne Nelson, Charles Porter, and Kory Fierstine, *RPED: A New Rapid Prototyping Strategy in the Department of the Navy,* CNA Research Memorandum DRM-2017-U-014757-Final, March 2017.

once formidable DOD R&D budget is increasingly dwarfed by that of the commercial technology sector. In terms of both time and resource considerations, DOD can't compete.

At the same time, other countries with global aspirations are doubling down on their development of technology for military applications, and introducing innovations to better leverage commercial technological developments. As stated by former Secretary of Defense Chuck Hagel, "While we spent over a decade focused on grinding stability operations, countries like Russia and China have been heavily investing in military modernization programs to blunt our military's technological edge."[22] Chief of Naval Operations ADM John M. Richardson echoed this concern: "Now that we're competing, we've got to make sure that we compete not only in capability, not only in capacity, but we also have to compete in time."[23] Failure to maintain such an edge diminishes the ability to the U.S. to deter conflict, threatens its effectiveness in the battlefield against technologically advanced foes, and endangers alliances and partnerships with countries relying on U.S. military strength. The ability of the U.S. military to retain a technological edge in this new environment is critical to its pursuit of national interests.

First mover or fast follower?

How can the U.S. military retain its technological edge in practice? Its current situation has analogs in the commercial sector. Consider the following examples:

First Mover	Fast Follower	Product
AltaVista	Google	Search Engine
Napster	iTunes	Music Downloads
Lotus123	Excel	Spreadsheet software
Motorola	Samsung	Mobile phones
Samsung	Apple	Smart Watches

[22] Hagel, keynote speech.

[23] Interview with CNO ADM John Richardson, Defense One, January 17, 2017. http://www.defenseone.com/ideas/2017/01/watch-d-brief-live-interview-chief-naval-operations-adm-john-richardson/134893/.

In each of these examples, the first company made investments and established an early lead in technological innovation. But over time, the company failed to leverage this early lead to become the dominant industry leader. Instead, these "first movers" were eclipsed by rivals that were able to take over their market share. These examples are not the exception: a University of Southern California study showed that almost half of product pioneer businesses failed, and the ones that did not tended to have smaller market shares than companies that entered the market later.[24] These first companies have been described as "first movers" (where an organization innovates and fields a new product) and the successors as "fast followers" (where an organization refines ideas from elsewhere and quickly adapts them). Though there are some notable examples of first movers achieving long-term success (e.g., Coca Cola, Hoover), the data show that long term success in business is more likely from a fast-follower approach than a first mover approach. This trend is stronger in an environment characterized by rapid innovation.

Leading versus winning the race

DOD is constantly challenged to stay abreast of current technological developments. Systems designed with cutting-edge technological capabilities, especially in the IT sector, are several generations behind current developments by the time they are fielded. In some areas, this lag in capabilities is acceptable, because it provides stability and predictability in areas where cutting-edge capabilities are not required. Yet in areas leveraging the strength of autonomy and artificial intelligence, this means a significant loss in capabilities from what could potentially be realized.

In this new environment of rapid innovation and significant R&D in the commercial sector, the edge the U.S. military currently has over other states in terms of military capabilities is fragile. Other States no longer require a significant R&D budget to develop their own organic capabilities with respect to autonomy and AI. Instead, they can glean from commercial innovation in other states and incorporate it into their own capabilities. This represents a paradigm shift of sorts: instead of high-end military capabilities being restricted to a small number of states that could afford the considerable R&D required to field them, in this new commercial sector–driven environment, there's a competition among states to see which one can quickly and effectively harness commercial developments into military capabilities. Such competition rewards the state that can become the most effective fast follower. So, how can the U.S. be an effective fast follower? What roles and capabilities does the U.S. military require to be successful in this technological competition?

[24] Steve Blank, "You're Better Off Being a Fast Follower than an Originator," Business Insider, October 5, 2010, http://www.businessinsider.com/youre-better-off-being-a-fast-follower-than-an-originator-2010-10.

A fast follower *follows*

A key characteristic of a fast follower is that it *Follows* current developments closely. For a military, this doesn't mean that it simply follows current overall trends in autonomy and AI, such as the general advances in machine learning exhibited by DeepMind's Go victories. Rather, the U.S. military needs to have a specific understanding of potential contributions that autonomy and AI can make to the military mission, as well as deep expertise in these technical areas to be able to recognize opportunities for leveraging developments as they arise.

The understanding and deep expertise is inherent in some military sectors. For example, in advanced electronics, priorities for development include some areas where DOD R&D is the chief effort (e.g., reconfigurable, frequency agile devices and circuits) and other areas that take a fast-follower posture (e.g., 3D Integrated Circuit Technologies) in recognition of the significant commercial development efforts taking place that can be leveraged.[25] This specificity in requirements involves more work up front to identify specific technology areas that enable specific military capabilities central to execution of the Third Offset strategy; yet they allow more careful monitoring of commercial developments that will help address those requirements. Just as DOD has identified key gaps and requirements in advanced hardware, it must do the same for specific aspects of autonomy and AI. This requires experts in these fields. Business experts studying successful fast followers have noted that being a fast follower requires an expertise as deep as that of the innovator, but that expertise will be employed in different ways—that then work in concert with system developers and operators, both to identify gaps and develop ways to integrate solutions to rapidly realize benefits.

A fast follower is *fast*

The other key component of being a fast follower is being *Fast*, which is not DOD's forte with respect to acquisition. A senior staffer on the Senate Armed Services Committee, Bill Greenwalt, observed: "The defense acquisition system is like an 18th century wooden warship that has been out to sea for too long, accumulating such a

[25] Dr. Gerald M. Borsuk, chair, Advanced Electronics COI, presentation at the National Defense Industrial Association Science and Engineering Technology Conference, April 13, 2016, Tampa, FL.

surfeit of barnacles that it can barely float, let alone operate under full speed."[26] As mentioned before, both DOD and Congress have a set of policies and laws that collectively slow the acquisition process.

Changing this situation is inherently risky: many organizations tend to take on slow processes out of a desire to reduce risk. There was a common saying in business not so long ago: "Nobody ever got fired for buying IBM." The quip suggested that a company's purchasers would typically buy more expensive IBM equipment, because if the equipment failed they could blame IBM. But if a less expensive option was chosen, then the purchasers could be blamed.[27] A decision that minimizes risk but carries opportunity costs can be a favored choice when incentives penalize rather than reward risk taking. The same phenomenon is also seen in the Intelligence Community, which can tend to exaggerate the magnitude of threats, since there can be serious consequences of underestimating the risk of a threat if that threat is realized, but there are often no consequences from overestimating a threat.[28]

For an organization to be an effective fast follower, it must adjust its calculus for managing risk. The adjustments include creating more incentives that reward risk taking and speed, and not short circuiting the intentional process of weighing costs and opportunities objectively by defaulting to slower, less risky processes. This is especially the case for technological fields dominated by the commercial sector, because the slow bureaucratic processes involved in DOD acquisition are a disincentive for fast-moving commercial technological companies. The culture in these companies typically involves quick decisions and a willingness to commit, while working with DOD can involve months to years with an open bidding process and no guarantee of success. Because of this, the slow, rigid nature of the acquisition process carries a double penalty in areas of fast-moving technologies.

One exception to this slow process is the Urgent Operational Needs System (UONS). Early on in Operation Enduring Freedom (beginning in 2001) and Operation Iraqi Freedom (beginning in 2003), operational challenges were recognized that did not have an established capability to address them. A number of processes at the Service and joint levels were created to streamline potential solutions to meet the urgent

[26] William C. Greenwalt, "Scraping off the barnacles of the defense acquisition system," AEI, October 15, 2014, http://www.aei.org/publication/scraping-barnacles-defense-acquisition-system/ print/.

[27] Scott Alan Miller, "No One Ever Got Fired for Buying…," SMB IT Journal October 17, 2016, http://www.smbitjournal.com/2016/10/no-one-ever-got-fired-for-buying/.

[28] Greg Thielmann, "Intelligence in Preventative Military Strategy," in William W. Keller and Gordon R. Mitchell, eds., *Hitting First: Preventative Force in U.S. Security Strategy* (Pittsburg, PA: University of Pittsburg Press, 2006).

operational needs. These needs were identified by tactical forces and operational commanders, then were met quickly when possible with commercial off-the-shelf technology (COTS) or developmental systems. Inherent in this process is an acceptance of greater risk. For example, U.S. Central Command (CENTCOM) described how for some of these needs, "a 51-percent solution is good enough."[29] These solutions needed to meet only minimum safety requirements and be judged suitable to address the submitted request. A number of important capabilities were fielded in this manner, including counter–improvised explosive device (IED) and counter-mortar defensive capabilities. However, because of the rapid nature of the fielding, there were a number of critical longer-term questions that were not resolved with these systems, such as lack of training, developing effective concepts of operations (CONOPS), and how they would be sustained in the field.[30] These rapid deployments of emerging capabilities also tended to increase the footprint of contractors on the battlefield, as their support was often required to make these capabilities function in a combat environment. Also, previous CNA work observed that when these systems meet enduring requirements, the transition from rapid acquisition processes to deliberate ones has not been consistently successful.[31]

Notably, this process only supports urgent requirements identified in current operations. When DOD reaches the point where it can acquire AI and autonomous capabilities in COTS or by fielding developmental systems, the question of risk in such potential deployments will need to be considered carefully, since such considerations are not normally part of the UONS process.

[29] Eileen Whaley and Dana Stewart, "Path from Urgent Operational Need to Program of Effort," *Defense ARJ* 21, no. 2 (April 2014): 525–564, http://dau.dodlive.mil/2014/04/01/path-from-urgent-operational-need-to-program-of-record-2/#more-409.

[30] Defense Science Board, *Report of the Defense Science Board Summer Study on Autonomy,* Washington, DC: Office of the Secretary of Defense, June 2016, https://www.hsdl.org/?view&did=794641.

[31] Michael Stumborg, *Finding the Off Ramp after a Decade of Rapid Acquisition,* CNA Research Memorandum DRM-2016-U-014007-Final, August 2016.

Recent DOD innovations in acquisition

In the past few years, DOD has recognized the need for greater innovation and responsiveness in its acquisition processes and created several new organizations to begin to address those deficiencies. Several important organizations in this regard are

- **Strategic Capabilities Office (SCO).** Created in 2012, the SCO imagines new applications of available technologies and fast-tracks their development, with an emphasis on innovation and surprise.[32] SCO is often referred to as the initial phase of DOD's Third Offset strategy. With an emphasis on near-term impacts, early changes achieved through SCO efforts include the addition of an offensive mission capability for the SM-6 missile (originally designed for air defense) and adding a maritime targeting capability for the Army's MGM-140 Army Tactical Missile System (ATACMS).[33] Many of the specific prototyping efforts by the office remain classified due to its purpose of strategic surprise.

- **Defense Innovation Unit Experimental (DIUx).** DIUx is a 40-person organization chartered to take emerging commercial innovations and funnel them to DOD. Created in 2015 and located in California's Silicon Valley, DIUx specializes in finding inventions developed in the private sector (with no consideration of military applications) and connecting them with potential military users. Companies submit concept white papers, and DIUx has the ability to rapidly fund (within 90 days) pilot projects using a new procurement authority in the 2016 National Defense Authorization Act.[34] These projects can then be taken on by various elements of DOD. The result has been rapid prototyping and incorporation of commercial technology in military applications such as refueling planning software in the Combined Air

[32] Cheryl Pellerin, "DOD Strategic Capabilities Office is Near-Term Part of Third Offset," DOD News, November 3, 2016, https://www.defense.gov/News/Article/Article/995438/dod-strategic-capabilities-office-is-near-term-part-of-third-offset/.

[33] Sydney J. Freedberg Jr., "Carter, Roper Unveil Army's New Ship-Killer Missile: ATACMS Upgrade," Breaking Defense, October 28, 2016, http://breakingdefense.com/2016/10/army-atacms-missile-will-kill-ships-secdef-carter/; Aaron Mehta, "Work: Munitions, Strategic Capabilities Office Boosted in FY18 Budget Plan," Defense News, December 5, 2016, https://www.defensenews.com/digital-show-dailies/reagan-defense-forum/2016/12/05/work-munitions-strategic-capabilities-office-boosted-in-fy18-budget-plan/.

[34] Fred Kaplan, "The Pentagon's Innovation Experiment," MIT Technology Review, December 19, 2016, https://www.technologyreview.com/s/603084/the-pentagons-innovation-experiment/; https://www.diux.mil/.

Operations Center in Qatar, and autonomous drones searching caves for individuals in applications for Special Forces.[35]

- **Algorithmic Warfare Cross-Functional Team (AWCFT).** DOD recently established the AWCFT, chartered to "turn the enormous volume of data available to DOD into actionable intelligence and insight at speed."[36] Its first initiative is Project Maven, which has the goal of improving processing, exploitation, and dissemination (PED) of intelligence feeds through the use of machine learning. This effort devotes considerable resources to better supporting current operations through rapid exploitation of full-motion video.

Collectively, these DOD efforts aim to meet current and projected operational needs through increased use of artificial intelligence and autonomous capabilities. Notably, they all do this by working around the traditional DOD acquisition process.

Effective fast following: remaining gaps

These new organizations have helped to field new innovative capabilities in the near term. This is an important and valuable function, but DOD being a fast follower of commercial technological developments is more than looking to the commercial sector for specific opportunities for prototyping. Rather, being a fast follower also requires a more robust process of looking at specific requirements for technological capabilities, how they can be militarized (e.g., how they could fit into components of existing systems and those in development), and then carefully monitoring commercial technological developments to identify ways these requirements can be met.

Of course, there will be some types of programs and applications where DOD R&D will be critical, such as military unique applications such as tanks, military ships, and munitions. But autonomy and AI represent a critical area where commercial R&D can

[35] Dan Lamothe, "The Pentagon has tried to get Silicon Valley on its side for years. Now it's part of the air war against ISIS," *Washington Post,* July 19, 2017, https://www.washingtonpost.com/news/checkpoint/wp/2017/07/19/the-pentagon-has-tried-to-get-silicon-valley-on-its-side-for-years-now-its-part-of-the-air-war-against-isis/?utm_term=.c6f29404d2e8; Mark Wallace, "How Veterans Turned Entrepreneurs Are Disrupting The Pentagon's Weapons Program," Fast Company, April 3, 2017, https://www.fastcompany.com/40401930/how-military-veterans-turned-entrepreneurs-are-disrupting-the-pentagons-weapons-program.

[36] Deputy Secretary of Defense, memorandum, "Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)," April 26, 2017.

offer considerable developments. Adopting a fast follower posture in these areas means that those will be specific areas where DOD spends less R&D resources, but it will still require technical expertise in those areas: DOD will need to maintain technical experts to actively monitor technical accomplishments in these areas and look for ways these developments can be leveraged. This is not a trivial matter: government organizations tend to have disincentives for maintaining personnel with high levels of technical expertise; these disincentives will need to be overcome to maintain such experts.[37] These focus areas can also be shared with the commercial sector to incentivize industry to meet priority technology requirements. DOD can then prioritize its R&D resources for specific areas of autonomy and AI, which may be complementary or unique to work being done in commercial R&D efforts. At the same time, this effort is not just technical in nature: it also requires a deep knowledge of the expected operating environment, concept of operations, and expected challenges U.S. forces will face.[38]

As stated earlier, because of the rapid development of AI and autonomous capabilities in the private sector, the application of these technologies to military operations creates a competition for the U.S. with other states also seeking a military edge. Thus it is important for the U.S. military to be aware of these developments, including tracking technological advances in the militarization of autonomy and artificial intelligence by states such as Russia, China, Iran, and North Korea, and nonstate actors such as ISIS. The U.S. should monitor both emerging technical capabilities and envisioned CONOPS, including any plans for counter-offsets they may be developing. This understanding of developments by others can then be used in examining relevant operational plans, and determining how existing plans may need to be modified in light of these developments. This should also lead to identification of new military capabilities that might be required in light of these modified operational plans. In addition, the U.S. military can learn from organizational innovations other states have put in place to improve their own rapid and effective development and fielding of autonomy and AI.

Current DOD efforts to develop prototypes (SCO, DIUx) and harnessing strengths of machine learning in support of real-world operations are initial efforts in developing near-term capability in an area where DOD lacks significant experience or expertise.

[37] An instructive case study is the incorporation of technical experts from the U.S. Arms Control and Disarmament Agency (ACDA) into the State Department. A decade later, that technical expertise has largely eroded. Leon Ratz, *Organizing for Arms Control: The National Security Implications of the Loss of an Independent Arms Control Agency*. Project on Managing the Atom Discussion Paper #2013-06, Belfer Center for Science and International Affairs/JFK School of Government, September 2013.

[38] David Pearson, "The Fast Follower: Coming Up Behind Development Leaders," *Defense AT&L*, May–June 2015, https://www.dau.mil/library/defense-atl/DATLFiles/May-Jun2015/Pearson.pdf

But they can be improved. To get the most out of these efforts, they should be accompanied by in-stride learning efforts to provide feedback on the direction and nature of these initiatives. This is similar to work CNA conducted in support of current operations over the span of a decade, in concert with U.S. Joint Forces Command (JFCOM). For example, for Project Maven—in parallel to the current effort to improve the processing, exploitation, and dissemination of full-motion video—a similar effort can identify lessons regarding other applications that are amenable to machine-learning techniques and what larger technology, manning, training, and data requirements are called for. Such an approach can help improve the effectiveness of DOD efforts to apply autonomy and AI to urgent operational needs.

There is also a real tension between the goal of rapid acquisition of autonomy and AI capabilities and the other requirements that accompany such capabilities. Such acquisitions are done in ways to be effective and interoperable, and can be trusted appropriately based on their actual performance. Hence the actions discussed here should be accompanied by parallel efforts in these other areas, discussed in the following three sections. These actions include a new Test and Evaluation (T&E) process, end-to-end operational assessments, placing specific requirements on the senior review process in accordance with the DOD Directive on autonomy, and a host of actions designed to develop appropriate trust of these systems.

Recommendations

Build DOD technical expertise. Cultivate technical expertise on autonomy and AI in the military services capable of identifying specific technical requirements needed for achieving military capabilities. This includes addressing organizational disincentives for maintaining personnel with high levels of technical expertise.

Prioritize military R&D resources, leveraging a fast-follower approach. Instead of trying to cover all aspects of autonomy and AI, prioritize R&D resources to areas of the highest importance, or to areas not receiving attention in the commercial sector.

Monitor and integrate specific commercial developments. DOD technical expertise should track targeted autonomy and AI developments in the commercial sector, looking for ways to rapidly integrate those developments into military systems. These needs should also be advertised to industry to encourage their research and development in these areas

Track developments by others. Track technological developments towards militarization of autonomy and artificial intelligence by key states and nonstate actors, leveraging them for evaluation of U.S. operational plans, needed U.S. capabilities, and possible ways the U.S. can learn from these other efforts.

Introduce a learning loop. Conduct in-stride learning efforts for existing DOD innovation initiatives (e.g., Project Maven) in order to make efforts meeting urgent operational needs through autonomy and AI more effective.

Promoting interoperability in autonomous systems

Autonomous systems can be designed to have different types of relationships with their human counterparts. Some systems will be designed to be tightly coupled with humans: for example, where an autonomous system assists human operators in decision making or in processing and exploiting sensor data. These tightly coupled systems will tend to be used in situations that pose relatively less risk to the human operator.[39] In contrast, other systems will be designed to be loosely coupled with humans in situations of higher risk: for example, an autonomous air vehicle operating inside contested airspace.[40]

Regardless of the specific type of relationship an autonomous system may have with humans, there will still be some requirement for integration and interoperability with the rest of the military force. Autonomy in a military context does not mean full and complete independence but, rather, independence that is limited to the conduct of specific functions. Before and/or after those functions are completed, there is still a requirement for that platform to exchange information with the larger force.[41] The 2012 Defense Science Board report echoed this sentiment, noting "there are no fully autonomous systems just as there are no fully autonomous soldiers, sailors, airmen or Marines."[42] While not exclusively focused on autonomy, a related commitment to integration from DOD is contained in its Unmanned Systems Integrated Roadmap:

[39] For example, human-machine collaboration to improve the quality and speed of decision making. Sydney J. Freedberg Jr., "Centaur Army: Bob Work, Robotics, and the Third Offset Strategy," Breaking Defense, November 9, 2015, http://breakingdefense.com/2015/11/centaur-army-bob-work-robotics-the-third-offset-strategy/.

[40] Department of Defense Research and Engineering, *Technical Assessment: Autonomy,* Washington, DC: Office of Technical Intelligence, Office of the Assistant Secretary for Research and Engineering, February 2015, http://www.defenseinnovationmarketplace.mil/resources/OTI_TechnicalAssessment-AutonomyPublicRelease_vF.pdf. This report uses the concept of loosely coupled and tightly coupled autonomous systems.

[41] Ibid.

[42] Defense Science Board, *The Role of Autonomy in DOD Systems,* Washington, DC: Office of the Secretary of Defense, July 2012, https://fas.org/irp/agency/dod/dsb/autonomy.pdf.

"DOD will develop and field affordable, flexible, *interoperable, integrated,* and technologically advanced unmanned capabilities."[43]

As the U.S. military has become more and more of a networked force over the past few decades, it has become increasingly evident that such information exchange, often referred to as *interoperability,* is not a trivial matter. Rather, the U.S. military faces chronic challenges with effectively making an individual weapon system platform interoperable with the larger force. As observed in testing, military exercises, and real-world operations, poor interoperability both compromises mission success (e.g., allowing adversaries to penetrate defenses and engage U.S. forces) and leads to greater risk of inadvertent engagements (e.g., friendly fire and civilian casualties). This difficulty in achieving interoperability also slows the fielding of military capabilities, since systems are often not fully effective when they are first declared initially operationally capable (IOC). Rather, systems can require software updates, modified tactics, and training to work around observed deficiencies, and years may pass before deficiencies are fully remedied, if indeed they are at all.[44]

This section examines common interoperability challenges facing the Navy and the Joint Force, how they can apply to autonomous weapon systems, and ways to address those challenges to allow more rapid development and fielding, while also making those systems more effective through improved interoperability with the larger force.

A brief history of interoperability challenges

A history of integration and interoperability in U.S. operations shows the enduring challenge of U.S. military elements operating as a single, cohesive force. The U.S. military in the early 1980s pursued unified communications capabilities and networks to tie together largely independent military services in light of developments for the Second Offset, as well as for the "AirLand Battle" concept in the 1970s.[45] The failed Iran hostage rescue, Operation Desert Claw, was another

[43] *Unmanned Systems Integrated Roadmap, FY2013–2038,* Washington, DC: Office of the Secretary of Defense, 2013, p. 1 (emphasis added), https://www.defense.gov/Portals/1/Documents/pubs/DOD-USRM-2013.pdf.

[44] Larry Lewis, "Death by 1,000 Ant Bites," CNA briefing to Chief of Naval Operations, Washington, DC, May 17, 2006.

[45] The "AirLand Battle" concept stressed ground forces and air forces acting in concert against both an enemy front line and forces acting in reserve to prevent or slow replenishment and ensure victory.

strong impetus for this effort.[46] Unfortunately, as system capabilities became more advanced, this did not alleviate the interoperability challenges but, rather, changed their character, as some problems were remedied and new ones began to dominate. This evolution of force integration challenges can be seen in a review of some major U.S. operations over the past 35 years. CNA has analyzed interoperability challenges facing U.S. forces since Operation Desert Storm: this section includes findings from that body of work.

Grenada (1983)

These early efforts to better integrate the different military services and make them interoperable were put to the test in the U.S. invasion of Grenada in 1983. Unfortunately these early efforts were seen to be inadequate:

> The final challenge to invading forces was the lack of a fully integrated, interoperable communications system.… Communications was to have been the glue that would tie together the operation of the four independent United States military service elements. Unfortunately, communications support failed in meeting certain aspects of the mission.… For example, uncoordinated use of radio frequencies caused a lack of interservice communications except through offshore relay stations and prevented radio communications between Marines in the north and Army Rangers in the south. As such, interservice communication was prevented, except through offshore relay stations, and kept Marine commanders unaware for too long that Rangers were pinned down without adequate armor. In a second incident, it was reported that one member of the invasion force placed a long distance, commercial telephone call to Fort Bragg, N.C., to obtain C-130 gunship support for his unit which was under fire.…[47]

[46] Richard A. Radvanyi, "Operation Eagle Claw: Lessons Learned" (unpublished thesis), United States Marine Corps Command and Staff College, 2000.

[47] Stephen Anno and William E. Einspahr, "The Grenada Invasion," in *Command and Control Lessons Learned: Iranian Rescue, Falklands Conflict, Grenada Invasion, Libya Raid.* Air War College Research Report AU-AWC-88-043 (Maxwell Air Force Base, Ala.: Air University Press, 1988); reprinted as an extract from the original report by the U.S. Naval War College Operations Department, NWC 2082, 40, 42 (on-line, http://www.fas.org/man/dod-101/ops/urgent_fury.Htm ,

Operation Desert Storm (1991)

Efforts to make different services and systems interoperate together were strengthened after the 1986 Goldwater–Nichols Department of Defense Reorganization Act, which stressed integration of the different services to become more joint. Interoperability failures in Grenada were one impetus for this effort. This initiative had its first major operational test in Operation Desert Storm in 1991, showing some success as Iraqi elements were targeted effectively and with great precision. As described by former Deputy Defense Secretary Robert Work, "the Iraqi heavy formations built on the Soviet model were virtually reduced to an array of targets."[48] However, interoperability in Desert Storm was far from perfect. Army platoon leaders noted that their radios were incompatible with artillery squads, which complicated their requests for fire support.[49] Likewise, the effectiveness of air defense surveillance was hindered by poor connectivity and not all air defense platforms operating on the same network.

Concerted interoperability efforts after Desert Storm (1992–2002)

In Desert Storm, the military Services tended to use different operating areas to reduce the risk of friendly fire in light of known challenges in working together. This was also the case for Coalition partners. After Desert Storm, there was interest in having the Services be able to operate in the same areas and cooperate instead of simply deconflict. This impetus was strengthened by the fact that a significant fraction of U.S. casualties in Desert Storm were caused by friendly fire, where important information about friendly forces was not passed as needed. This resulted in the creation of the Joint Air Defense Operations Joint Engagement Zone (JADOJEZ) Joint Test and Evaluation Activity, which pushed capabilities and tactics to promote the ability of air defense systems to work together in a seamless battlespace. This activity was institutionalized as the All-Service Combat Identification Evaluation Team (ASCIET), later changed to Joint (JCIET), and its activities expanded to also cover ground operations and time-sensitive targeting and close air support. Due to the efforts of the services and joint initiatives such as this,

[48] Cheryl Pellerin, "DOD Seeks Novel Ideas to Shape Its Technological Future," DOD News, February 24, 2015, https://www.defense.gov/News/Article/Article/604159/dod-seeks-novel-ideas-to-shape-its-technological-future/.

[49] Sterling D. Sessions and Carl R. Jones, *Interoperability: A Desert Storm Case Study,* McNair Paper 18, Washington, DC: National Defense University/Institute for National Strategic Studies, July 1993, http://www.dtic.mil/dtic/tr/fulltext/u2/a271674.pdf.

interoperability challenges observed in Desert Storm were improved significantly, and exercises showed mission effectiveness benefits from this progress.[50]

Operation Iraqi Freedom and recent military exercises (2003–present)

New, network-enabled capabilities and tactics developed during the post-Desert Storm period were used in Operation Iraqi Freedom in 2003. Interoperability deficiencies observed in 1991, such as connectivity issues on the use of the tactical data link Link 11, were improved by moving to the more modern and robust Link 16. But this progress exposed another layer of interoperability challenges. Now that the systems could communicate, they experienced different kinds of interoperability problems, illustrating that network connectivity in itself did not equal interoperability. The problem was seen in joint exercises, where interoperability deficiencies degraded the collective force's operating picture, leading to confusion, inadvertent engagements (friendly fire and noncombatant casualties), and missed opportunities (i.e., leakers—enemies penetrating the defensive shield of U.S. forces).

Many of these same deficiencies were seen in Operation Iraqi Freedom. For example, in the Patriot missile system shoot-down of a Navy F/A-18C, different surveillance platforms were reporting different information regarding the aircraft, but that information was never fused in a coherent picture. Similarly, these platforms saw different pictures of the situation, reducing the ability of operators to sort out what the true situation was.[51] While some deficiencies from Operation Iraqi Freedom have been addressed, many others have not, and new deficiencies have also surfaced as systems implement newer combat system software. Hence, these same kinds of interoperability challenges continue to be seen in recent military exercises.[52]

[50] Lawrence Lewis, Jay Smith, Timothy Roberts, Bruce Behrens, and Paul Symborski, *Performance of the Integrated Air Defense System at JCIET 02: SIAP, Interoperability, and Operational Considerations,* CNA Research Memorandum D0007309.02-Final, December 2002, //Secret. (Portion cited here is unclassified.).

[51] Larry Lewis, "Improving Joint C2: Lessons from Iraq," presentation at the SMI Network-Centric Warfare Conference, 2008.

[52] Carla Barrett, "Interoperability in DOD: Why is it so hard to attain?" PowerPoint presentation, May 15, 2014.

Root causes for interoperability failures

The specific technical causes of interoperability challenges are myriad, and seemingly inconsequential interoperability problems have contributed to operationally significant events, leading to the observation that interoperability failures represent "death by a thousand ant bites." Supported by extensive data collection, these failures have been studied carefully. Based on CNA reconstruction and analysis of operations and exercises over the past 20 years, the many causes of interoperability challenges can be summarized in a few categories:

- Multiple networks and gateways
- Unmet or poor interface standards
- Platform-centric requirements
- Poor training and underdeveloped CONOPS

Multiple networks and gateways

A principal limitation to interoperability is that not all systems are on the same network. One reason for this is the creation and use of proprietary or Service-specific networks not sharing capabilities. These disparate networks understandably complicate information exchange. Introducing gateways that move information from one network to another is one remedy that has been used in some cases. However, experience with these gateways shows that they can be only a partial fix, plagued by missing information and latency problems.

Unmet or poor interface standards

Even when systems are on the same networks, this alone does not ensure interoperability. Systems can be operating together on a particular network and still experience problems operating effectively. For example, networks and data links have implementation standards that govern the format and processing of messages. If systems do not comply with those standards, then messages will not be processed as intended, leading to problems. Sometimes this happens because system Program Offices make implementation errors; other times, there is ambiguity in the standards that allow for different implementation. Also, when changes are made to the standards, lack of coordinated implementation of those changes can also lead to non-interoperable systems.

Platform-centric requirements

These two interoperability challenges tend to be symptoms of a single cause: a DOD acquisition process that is platform-centric.[53] In this process, system Program Offices develop system requirements, and these requirements often focus on single system performance. Individual Program Offices make implementation decisions regarding network compatibility and combat system design. These implementation decisions are largely uncoordinated and, collectively, differences in these decisions hobble interoperability across the force. There is no forcing function for driving needed changes. Often, either specific system-level requirements for interoperability with the larger force are not sufficient, or fiscal limitations of the program introduce a cut line for meeting requirements, and those for interoperability fall below the line. For example, when asked about these interoperability requirements, one System Program Office stated that they were its "highest unfunded priority."

Training and process challenges

Training and operational processes can also create interoperability challenges. For example, in the 2003 Patriot missile shoot-down of a Navy F/A-18C and a UK GR-4, in addition to technical issues, the operators were not trained to evaluate the weapons system.[54] Also, for Predator and Reaper, the operational process for processing, exploitating, and disseminating allows communication breakdowns that limit effective information sharing regarding the engagement of targets. Information available to the imagery analyst watching the full-motion video was not consistently and accurately communicated through the UAV crew to the command authority making the engagement decision.[55]

Summary

Interoperability challenges have shifted from not having integrated communications to communications that were uncoordinated. Uneven implementation decisions by different Program Offices also detracted from interoperability. These deficiencies have been seen numerous times in military exercises; they were also seen in real-

[53] Marsha Mullins, "Joint Force Digital Interoperability Remains Elusive," *Signal,* October 1, 2014, https://www.afcea.org/content/joint-force-digital-interoperability-remains-elusive.

[54] Larry Lewis, *Operation Iraqi Freedom: Ground-to-Air Fratricide* (U). CNA Research Memorandum CRM D0008910.A4, July 2004, //Secret. (Portion cited here is unclassified.)

[55] Larry Lewis and Sarah Holewinski, "Changing of the Guard: Civilian Protection for an Evolving Military," *Prism* 4, no. 2 (2013).

world operations such as major combat operations in Iraq in 2003. The common operational picture had many deficiencies, and most friendly fire incidents had an interoperability contribution.

Increased demands on interoperability for autonomy

Some could argue that these considerations are less important for autonomous systems, since they are performing functions independently. But, as stated earlier in this section, this doesn't mean that these systems do not need information from outside sources. In fact, autonomous systems could be more vulnerable to interoperability challenges for several reasons:

- **Potentially fewer communication opportunities because of autonomous operation.** In practice, interoperability breakdowns tend to be corrected over time as differences are arbitrated and resolved. But this requires continuing communication over time. A limited time window for communication can miss this self-correcting effect.

- **Lack of a human operator to override potential problems.** Autonomous systems will be designed to consider many elements of information in making decisions. However, sometimes there is conflicting information available that complicates a decision. In some situations (for example, the standards for Link 16), human operators are required to be alerted to these situations in order to resolve them. This requirement is clearly problematic for an autonomous system, so this situation will need to be addressed in interface standards and systems. And sometimes the data do not seem to conflict but instead appear to suggest what is actually not the case. One example of this was USS *Valley Forge* during Iraq operations in 2003. One day, an aircraft—unidentified on the shared data link and not replying to interrogations of Identification Friend or Foe (IFF) Mode 4—was observed closing on the ship's position. It appeared to be a threatening profile, and the ship prepared to fire at the aircraft in self-defense. Though the engagement met the rules of engagement (ROE), the commanding officer finally decided to not shoot, being uncomfortable with the situation. It was later discovered that the aircraft was a Navy F-14, illustrating the value of human judgment.[56]

[56] Lewis, *Operation Iraqi Freedom.*

- **Managing risk from a** more **agile acquisition process.** As noted in the previous chapter, DOD will need to have the ability to more rapidly incorporate technological capabilities in this new competitive environment. This will require additional efforts to manage increased risks of interoperability challenges due to a more compressed timeline.

What these things mean for autonomous systems is that any communication opportunity needs to be particularly effective—there may be no second chance to correct the information sent previously, and there is no opportunity for human operators to apply their intuition and step in when something seems wrong. At the same time, this careful engineering process must be done in a more compressed timeframe than is done today for legacy systems. Two questions are helpful to answer in light of this increased risk: what specific types of information will lethal autonomous systems require, and how can those information requirements be met in ways that are effective and interoperable?

What type of information will lethal autonomous systems require?

While autonomous systems are able to make key decisions without human input, this does not mean that these systems are stand-alone. Specific requirements for interoperability will depend at least in part on the mission and the autonomous functions given to that system. For example, a weapon system using lethal autonomy—with functions including mission tasking, target development, target identification, developing situational awareness, and target deconfliction—will still require some level of interaction and interoperability with the larger force. As a starting point, specific information needed for these functions includes

- Mission guidance (e.g., commander's intent, ROE, planning information): initial guidance and any changes

- Situational awareness/friendly force locations (e.g., Forward Line of Own Troops, forward elements, Special Operations Forces, adversary locations, civilian population information, humanitarian/protected sites such as as hospitals)

- Last minute deconfliction information: for example, No Strike List of protected entities and their locations can and often does change on a daily basis. Some of these are very hard or infeasible to detect with military sensors, so procedural deconfliction is used as a safety net.

This reliance on information before the moment of the trigger pull is implicitly acknowledged in a DOD Directive on lethal autonomy, DODD 3000.09.[57] The Directive states that autonomous engagements will be informed by "appropriate human judgment". This wording implies that some form of outside input will inform the engagement decision. It is worthwhile to note that this wording is used deliberately instead of an alternate term, "meaningful human control." The latter is often used in international discussions regarding lethal autonomy, and tends to involve having a human decision maker involved in the final decision to use force. In contrast, the specific term used in the Directive recognizes that judicious use of force is not determined simply by having a human operator make a decision at the moment of the trigger pull, but is influenced by many factors, including broader situational awareness and a good understanding of the commander's intent. Clearly, these factors will need to be translated into rule sets that a machine can use. The different categories of information listed above are various ways that the human judgment called for in the DOD Directive can inform the use of lethal force by autonomous systems.

Meeting information requirements in effective and interoperable ways

Once information requirements for lethal autonomous systems are well understood, the design for these systems should deliberately include best practices of effective and interoperable communications for exchanging this information. Specific program offices designing and fielding autonomous weapon systems should develop a robust list of information requirements, akin to the list provided in the previous section, and ensure it is supported by communications capabilities. This should include learning lessons from the past: pursuing common architectures, making standards for data link implementation, and enforcing their implementation for applicable Program Offices. Enforcement of these requirements could be part of the senior review of fully autonomous systems required in DODD 3000.09.

The required Test and Evaluation process for these systems should aim to identify interoperability concerns. Yet invariably there are issues not observed in the T&E process that emerge in later exercises and operations. These can sometimes be tied to aspects of the operational environment—including the type of assets working together, the proximity of friendly and other platforms, and environmental conditions—that were not represented during original testing. Thus lethal autonomous systems should also be involved in periodic risk-reduction live events

[57] The timing and method of such communication will be challenged when these systems are operating in a communications-denied environment.

throughout the development life-cycle of these systems, using actual systems making constructive (virtual) engagements.[58]

A best practice for this dating back to the 1990s is to have extensive data collection and analysis, enabling replay of live sensor and system data overlaid with truth data such as GPS positions of entities. This process enabled a robust approach to identifying problems and then tracing them back to their root causes, allowing early identification and focused remediation of interoperability problems. These events and the follow-on analysis provide both early warning of potential deficiencies and opportunities to evaluate potential fixes. Collectively, these processes will help reduce the baseline of interoperability challenges while allowing an overall process to refine and improve systems over time. Such a risk reduction approach is particularly valuable in the increasingly competitive environment with autonomy and AI. In this new environment, there is a desire to increase the pace of development and fielding of these systems, leaving less time for testing and evaluation: there is a natural tension between rapid acquisition and taking steps to promote and ensure interoperability, increasing the likelihood of encountering interoperability challenges. Having risk-reduction events married with data collection and analysis would help to manage this risk. Also, this increases the opportunity to learn from failures, heeding Henry Ford's observation that "Failure is simply the opportunity to begin again, this time more intelligently."[59]

This data-and-analysis approach can also be married with experimentation. One of the essential elements of the Third Offset strategy is an exploration of alternatives and discovering what options give the most benefit. Joint Chiefs of Staff Vice Chairman Gen. Paul J. Selva put the matter thus: "From an operational perspective, the journey we're on has the potential to vastly increase the effectiveness of our conventional forces but we have to ask the right questions. We have to experiment with the right tactics, techniques and procedures."[60]

Experimenting with technology and tactics was also essential to the success of the Second Offset.[61] However, one challenge with experiments is that they can be evaluated subjectively. A lesson learned from exercises and even operations is that an operator's perception may seem to indicate success, but when the data are analyzed, that operator's perception is not always matched by the facts. For example,

[58] Mullins, "Joint Force Digital Interoperability Remains Elusive."

[59] Erika Andersen, "21 Quotes from Henry Ford on Business, Leadership, and Life," Forbes Magazine, May 31, 2013, https://www.forbes.com/sites/erikaandersen/2013/05/31/21-quotes-from-henry-ford-on-business-leadership-and-life/.

[60] Pellerin, "Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence."

[61] Perry, "Desert Storm and Deterrence."

at a conference in Bahrain after Operation Iraqi Freedom, air defense operators lauded the quality of the air picture during major combat operations. But the last presentation featured actual data showing problems in the picture that the operators were not aware of. This demonstrates that using data collection and analysis to supplement and confirm operator and observer impressions can help experimenters arrive at valid conclusions. They also give additional opportunity to determine the root cause of deficiencies and develop better solutions to those deficiencies, accelerating efforts to improve capabilities. Hence this data-driven analysis approach would be a valuable addition to planned experimentation efforts on autonomy and AI.

Recommendations

Programmatic focus on interoperability: program offices give close attention to interoperability for autonomous systems, especially for those using lethal force, given the greater vulnerability autonomous systems can have to interoperability challenges. These include

- Determining specific information requirements for the use of lethal autonomy
- Designing systems with communication capabilities to support these requirements
- Adopting best practices for interoperability: pursuing common architectures, making standards for data link implementation, and enforcing their implementation for applicable Program Offices.
- End-to-end interoperability testing, not simply interface format compliance tests.

Policy requirement for interoperability: Make a requirement for observing interoperability best practices as part of the senior review of fully autonomous systems required in DODD 3000.09.

Reduce risk through live events: Use regularly scheduled risk-reduction live events (such as exercises) throughout the development life-cycle of autonomous systems to reduce risk. This should include instrumented systems in operationally realistic environments in order to provide early warning of potential deficiencies and give opportunities to evaluate potential fixes.

Marry data and analysis with experimentation. Include data collection and analysis during experimentation events in order to supplement and confirm operator and observer impressions, and accelerate the process for improving capabilities overall.

Mitigating risk in lethal autonomy

Perhaps the most contentious question regarding the military use of autonomy is: Should autonomous weapon systems be allowed to use lethal force? The potential use of autonomy to deliver lethal force carries both potential benefits and potential risks. Potential benefits include enhanced military capabilities such as:

- Greater reaction speed against time-sensitive threats
- Expeditionary advantages—greater reach and endurance without human operators
- A possible option in communications-denied environments
- Force-protection, preventing troops from exposure to risks

Autonomy could also offer potential humanitarian/ethical benefits, including:

- Impartiality—no human weaknesses such as fear, anger, bias
- Capabilities that could enhance precision of target selection and weapon effects delivery
- Lower cost/risk of troop casualties, making humanitarian intervention more feasible
- Self-sacrifice of the autonomous platform to protect humans
- Asymmetries that could reduce the likelihood of war or lead to more rapid termination of conflicts.

At the same time, the use of autonomy in lethal force presents a number of potential risks that are humanitarian, ethical, and strategic in nature:

- An increased risk of fratricide
- Systems may not be able to comply with IHL, and may be prone to causing civilian casualties
- Lack of humanity: machines may be unable to show restraint and mercy

- Unable to ensure human/moral responsibility and accountability when a machine makes the decision to take a human life
- An autonomous arms race likely would require developing learning, adaptive systems, and the interaction of such systems on the battlefield, which could lead to unpredictable behavior and loss of human control
- Greater risk of proliferation and challenge of verification, because software is the key enabling technology
- Danger of undermining strategic dominance if strength on the battlefield increasingly depends on application of AI technologies that will become ubiquitous and cheaper on the commercial market
- Wars could become more prevalent, since the loss of troop casualties as a deterrent makes war more attractive
- Less technologically sophisticated opponents could be driven to extreme responses, in violation of international law
- Lack of reliance on humans to deliver force can empower dictators, terrorist groups, lone-wolf attacks, including weapons of mass destruction (WMD)–scale events

Different groups respond to these benefits and risks differently. In DOD's Third Offset, autonomous weapon systems are viewed as essential tools for national security. At the same time, some technologists and scientists, NGOs, and even some states view lethal autonomy as problematic for civilian protection and ethical considerations. Despite these different overall positions, both sides agree that the risks of bringing autonomy to the use of lethal force is something that requires additional scrutiny, especially in light of the accelerating pace of technology.

A key risk of lethal autonomy: unintended engagements

The risks of lethal autonomy range from proliferation of technology to changing the strategic balance of deterrence and causing war to be more likely. Yet the main area of scrutiny for lethal autonomy in international discussions has been the question of limiting weapon effects: can lethal autonomous weapon systems use force in such a way as to target the desired military objective and avoid unintended engagements, consistent with international law and avoiding negative outcomes such as civilian casualties? This section focuses on this key risk. While the other risks stated above

are also important to address, they are all complex topics in themselves, which will need to be analyzed and considered outside the scope of this report.

DOD policy on the acquisition and fielding of autonomous weapons addresses this primary concern directly, and specifically aims to avert "unintended engagements" by autonomous weapons through a senior-level review before such systems are developed or fielded.[62] While the directive does not specify the nature of these engagements, we identified three types of engagements that are unintended and have negative effects on the conduct of military operations: friendly fire, civilian casualties, and inadvertent engagements of other states' military forces. These engagements are all undesirable in themselves; they are also examples of tactical events that have strategic consequences. For example, friendly fire can cause divisions in a Coalition, slow the tempo of operations, and reduce trust among forces. Civilian casualties can hinder freedom of action and reduce the perceived legitimacy of a military's actions. Inadvertent engagements of other military platforms—especially when outside of a current armed conflict—can result in undesired escalation toward conflict, as well as undermining U.S. national objectives and freedom of action.

The U.S. military endeavors to use force consistent with both its legal requirements and its values and principles. At the same time, the U.S. military has suffered past inadvertent engagements and has sought to learn lessons from them. CNA has analyzed these types of inadvertent engagements and developed operational lessons. These lessons can inform safeguards, in both policy guidance such as the DOD Directive, and in broader technology, tactics, and doctrinal considerations to avoid unintended engagements by autonomous weapon systems.

Lessons from friendly fire

Friendly fire is the inadvertent engagement of one's own forces in armed conflict. It has received increased attention over the past 25 years as it made up an increasing proportion of U.S. casualties, in light of a sharp decrease in overall combat losses in recent conflicts. For example, in the 1990–91 Gulf War, 26 percent of total U.S. fatalities (38 of 148) were from friendly fire. Similarly, in Iraq major combat operations in 2003, 19 of 109 U.S. combat fatalities were from friendly fire (17 percent). Friendly fire from U.S. forces is also a risk for Coalition partners in combined operations. For instance, collectively from Operation Desert Storm and

[62] "… minimize the probability and consequences of failures in autonomous and semi-autonomous weapon systems that could lead to unintended engagements." DODD 3000.09.

Iraqi Freedom, 75 percent of UK casualties from friendly fire were caused by U.S. forces (12 out of 16).[63]

Over the past twenty years, CNA conducted a number of studies of friendly fire from U.S. operations, as well as simulated incidents during military exercises. This analysis identified a number of common themes that often contribute to the engagement of friendly forces:

- **Misidentification:** Friendly forces were seen as a threat based on behavior or misinterpreted information or intelligence. Behavior of individuals or vehicles was judged as hostile intent, and intelligence or measurement data was misinterpreted as corresponding to a threat.

- **Failure of Identification Friend or Foe (IFF):** The military has capabilities specifically designed to provide identification information in order to avert friendly fire, including Mode 5, combat identification panels, Link 16 Precise Participant Location Information (PPLI), and Infrared beacons. Yet in the majority of cases, when these measures were present, they failed to stop friendly fire events due to a combination of *system performance* problems and an *incompatibility between sensor and IFF method*.

    - ***System performance:*** IFF capabilities themselves were seen to be unreliable. For example, Mode 4 was seen to be unreliable in providing positive identification of aircraft in combat operations in Iraq. Its replacement, Mode 5, also appears to have performance challenges.

    - ***Incompatibility between sensor and IFF method:*** IFF measures did not provide protection when the shooter lacked the capability to detect them. For example, a friendly aircraft being reported on Link 16 is not protected when the shooter lacks Link 16 connectivity. Similarly, a friendly ground vehicle with an IR beacon is afforded no protection when the shooter is viewing the engagement through a sensor looking at the entire visual spectrum.

- **Identification not available at the shooter:** In friendly fire incidents observed in Iraq major combat operations, as well as in previous joint exercises, it was observed that someone in the joint force knew that the engaged friendly was a friend. However, that information was not passed to

[63] Larry Lewis and Paul R. Syms, *UK and U.S. Friendly Fire in Recent Combat Operations,* TTCP Technical Report DOC–JSA–AG13–3–2006, October 31, 2006.

the shooter. This situation points to the primary challenge of friendly fire not being the identification of friendly forces as a friend, but rather the effective sharing of that information with the rest of the joint force.

- **Poor situational awareness:** The shooter in friendly fire events often had poor situational awareness, unaware of either their own location or the location of other friendly forces (for example, not being aware of the location of the Forward Line of Own Troops (FLOT). This challenge was particularly pronounced for operators of highly automated systems, where operators were not trained to maintain situational awareness in general. As a result, they were not equipped to provide appropriate human judgment to automated decisions.

Lessons from civilian casualties

The United States takes great care in avoiding civilian casualties in war, consistent with its principles and values, as well as its legal obligations. Over the past ten years, the U.S. military requested a series of studies to better understand how civilian casualties occur in armed conflict, and what measures it could adopt so that it could more effectively reduce civilian casualties. CNA led these studies. Overall, U.S. forces complied with international humanitarian law (IHL, also known as the Law of Armed Conflict, or LOAC) in the vast majority of cases. However, this collective body of work led to a number of insights regarding how civilian casualties tend to occur in U.S. operations:

- **Unobserved civilians in the target area:** Civilian casualties can result from engagements where it is not believed that there are civilians present. This can occur when civilians move into the target area at the last minute, and it is too late to abort the attack. One example of this is in the aftermath of an attack: first responders move into the area unobserved to give medical aid, and are accidentally harmed by follow-on attacks. This can also happen in the case of attacks on vehicles or buildings, where civilians are present but are not visible to surveillance efforts.

- **Misidentification:** It was widely assumed that civilian casualties in military operations occur when an engagement is intended to be against a valid military target: the weapon effects hit the valid military target, but there were unobserved civilians in the area, and they were also harmed by the engagement. This “collateral damage” mechanism was the focus for U.S. military efforts to reduce civilian casualties before 2010. However, studies found that this mechanism applied only about half the time. The other half were cases of misidentification: U.S. forces engaged who they thought was a

valid military target but was actually misidentified civilians, resulting in civilian casualties. There are two primary mechanisms for misidentifications:

  - ***Misinterpretation of activity,*** where civilians are declared to be a threat based on perceived hostile intent or a hostile act; and

  - ***Misassociation with a valid military target:*** civilians are mistakenly declared to be combatants after a combatant merges with the civilians and the two groups are conflated, or alternately, civilians move into areas where combatants were known to operate per available intelligence and declared hostile based on that information.

- **Not exercising tactical patience when feasible:** tactical patience is an option when the conditions for using force are met per ROE and other guidance, but there is no immediate threat that requires actions in self-defense. In this case, U.S. forces can take more time in their decision process in order to avoid civilian casualties—for example, looking at available information, coordinating with others or changing their vantage point to get additional information, and considering pattern-of-life factors. There are many examples where taking such additional precautions averted mistaken engagements of civilian targets.

- **Unexploited opportunities for tactical alternatives:** Tactical alternatives are available when there are different options for using force to achieve the desired effects. For example, a unit that responds in self-defense by ordering an airstrike on a building from which a combatant is firing at friendly forces could consider other options for addressing the threat, such as using a sniper to engage the shooter.

Lessons for inadvertent engagements of adversary military forces

In addition to challenges of positive identification, discussed in the sections above, there is also a risk of an autonomous system engaging adversary military forces at times or in conditions where it is not appropriate. In some cases, those engagements could be contrary to international law; regardless of the engagements' legal status, they may also result in international condemnation and loss of legitimacy. This risk is managed through U.S. military ROE, which detail who and under what conditions may be the subject of the use of force in a particular conflict.

However, ROE are not static; they can change, sometimes rapidly, and they can change many times during the course of operations. After the end of major combat

operations in Iraq in 2003, the ROE changed many times to reflect the dynamic nature of the environment, and to reflect the intent and allegiances of various groups to the developing insurgency. A lessons-learned effort led by CNA observed that forces found themselves challenged to keep up with these multiple changes, complicating the consistent use of force. The following lesson is based on U.S. experiences in Iraq:

- **Avoiding inadvertent engagements of adversary military forces:** When using force, it is vital that U.S. forces maintain the current version of the ROE and the associated commander's guidance for the use of force. This information can include the current phase of the conflict, and whether the use of force is authorized overall, the various entities that constitute a valid military target, and other considerations regarding the use of force, including collateral damage criteria.

Developing senior review criteria

Currently, DODD 3000.09 requires a senior-level review for development and fielding autonomous systems, with the specified purpose of avoiding inadvertent engagements. To date, however, no system has met the criteria for such a review; so no senior-level review has ever been conducted. Furthermore, there is no discussion in the DOD Directive of the overall process or specific issues to be examined within the context of that review. The lessons stated above capture the primary causes of inadvertent engagements from the past 15 years of U.S. operations. Given that the purpose of the senior review is to avoid inadvertent engagements, it would be prudent for these reviews to include a check for these historical risk factors. In addition, it would be helpful for Program Offices working on autonomous systems to be aware of these risk factors in advance, so that system requirements and design can take these lessons into account. The lessons could be communicated by including these risk factors in the DOD Directive itself, or by the Office of the Secretary of Defense (OSD) providing separate implementing guidance to aid Program Offices seeking to comply with the DOD Directive.

Recommendations

The above set of lessons from inadvertent engagements suggests a number of recommendations for lethal autonomous weapon systems:

Monitor for misidentifications: Autonomous systems should give careful attention to the possibility of misidentification, including cross-checks of different kinds of identifying information and flagging potential conflicts or inconsistencies—for

example, identifying that an entity has kinematics that are inconsistent with a suspected platform or target type.

Include robust IFF measures: Sensors for autonomous systems should ensure compatibility with appropriate anti–friendly fire measures.

- For example, an autonomous system that is able to engage air targets could include Mode 5 or Link 16 PPLI. For ground targets, the autonomous system could include Blue Force Tracker (BFT) reception or sensors able to detect infrared (IR) signatures (strobes or panels).

- It should also be acknowledged that such systems have failed in the past as a single-source safety measure. Multiple measures are preferred when feasible; where they are not, a heightened risk of friendly fire should be understood.

- This consideration should also extend to humanitarian applications—for example, the Geneva Conventions call for hospitals to display red crosses/crescents to indicate their protected status; autonomous systems operating in areas where hospitals could be present should have the ability to distinguish such markings.

Leverage available information: Autonomous does not necessarily mean isolated. In light of mission requirements, autonomous systems should be provided with information and intelligence when possible to ensure current situational awareness and inform optimal engagement decisions. This should also include provision of current ROE and other guidance for the use of force to ensure engagements are consistent with commander's intent and applicable law.

Consider civilian casualties: Autonomous systems should give careful consideration and make every precaution to avoid civilian casualties, consistent with measures U.S. forces have put in place for recent operations. These measures include

- Compliance with IHL. This is a matter of extensive training for U.S. forces; autonomous systems must also be sure to comply with legal requirements for the use of force in armed conflict.[64]

- Not assuming that no civilians observed means no civilians present.

[64] This point is discussed in more detail in the report from the March 2014 Expert Meeting of the International Committee of the Red Cross: *Autonomous Weapon Systems: Technical, Military, Legal, and Humanitarian Aspects,* Geneva, Switzerland: ICRC, March 26–28, 2014, https://www.icrc.org/en/.../4221-002-autonomous-weapons-systems-full-report.pdf.

- Taking additional measures to screen for collateral damage, such as pattern of life determinations and zooming out the field of view to screen for civilians
- Exercising tactical patience when possible, and considering tactical alternatives

Develop DODD 3000.09 senior review criteria. These considerations should be made part of the required senior-level review for development and fielding of autonomous systems per DODD 3000.09.

Examine other risks of lethal autonomy. This report examines the risk of inadvertent engagements by lethal autonomous weapon systems. A further study should examine a number of other potential risks presented by lethal autonomy that are humanitarian, ethical, and strategic in nature.

Addressing concerns about lethal autonomy

For the First Offset, which used nuclear weapons as a deterrent against Soviet expansion, its deterrence value decreased over time as the feasibility of the U.S. nuclear option was increasingly put in question. Similarly, the value of autonomy and AI as a deterrent will be effective only if it is perceived to be a real option that can be employed.

Thus the U.S. has a real interest in making sure that it is able to employ autonomy and AI in operations if necessary to defend itself against critical threats. Previous sections have discussed challenges relating to military institutional and technical considerations: the acquisition process, making systems interoperable, and avoiding tragic consequences such as friendly fire and civilian casualties. But these technical considerations are only part of the equation with regard to the larger question of whether this capability can plausibly be used. The ability to use these capabilities also depends on overcoming human barriers, especially those based on how these systems are viewed. The barriers include whether operators and leaders trust these systems, whether our allies will agree to support Coalition operations when such systems are used, and international legal and normative frameworks. While not necessarily required for U.S. freedom of action, it could also be helpful in reducing the inherent mistrust of this technology through news and industry-related articles addressing questions such as “Should Autonomous Robots Kill?”

Autonomy in warfare, is likely inevitable. Yet the U.S. has an opportunity to help influence the forms autonomy will take and the purposes it will serve. Thus its implementation of the Third Offset can not only meet direct military objectives for the effective use of force, but also promote U.S. national interests consistent with its principles and values. As discussed later in this section, history has shown that this kind of approach can improve the perception of U.S. efforts, and has resulted in enhanced freedom of action.

U.S. military and government: appropriate trust in autonomy

A key question regarding the U.S. use of autonomy is whether the military and senior leaders trust that autonomous systems will be effective and not cause inadvertent problems. The topic of trust and autonomy has been addressed in depth in *AI, Robots and Swarms,* an earlier CNA report, as well as in other reports such as the 2016 Defense Science Board Summer Study on Autonomy. The CNA report in particular points out that there are myriad philosophies and approaches to the concept of trust—demonstrating that this is still an emerging field of study—then outlines various dimensions of trust and some key barriers to humans trusting in autonomous systems.[65]

A basic definition of trust is "assured reliance on the character, ability, strength, or truth of someone or something."[66] For military use of technology, the key terms in this definition are *reliance*, the willingness to use the technology, and *assured*, which points to a reasonable confidence that the technology can be relied on. How can the U.S. military construct military capabilities that are accompanied by the willingness and confidence to use them? There are two echelons that need to be considered here: operators and commanders who would need to use them operationally, and U.S. military and government senior leaders who would need to authorize their development, fielding, and use.

Operators and commanders

Commanders and operators responsible for a given operation are unlikely to authorize use of a system when they do not fully understand what the effects will be. The 2016 Defense Science Board study makes this point: "The individual making the decision to deploy a system on a given mission must trust the system."[67] This principle was seen consistently in Iraq and Afghanistan operations. In some cases, systems were fielded urgently—such as counter-IED systems or surveillance systems providing critical intelligence—and they were eagerly received and used extensively. However, there were other cases where tactical forces generally chose weapon systems and ISR platforms that they were already familiar with, even when superior but less familiar capabilities were available. This illustrates that, even though

[65] Ilachinski, *AI, Robots, and Swarms.*

[66] https://www.merriam-webster.com/dictionary/trust.

[67] Defense Science Board, *Summer Study on Autonomy.*

systems may be provided to operating forces in the field, it is not in itself a guarantee that they will be used.

Now, the non-usage of some systems was not insurmountable. In those operations, the challenge was addressed by proactive training on available systems and their capabilities (and limitations) prior to deployment. Some of these systems were also made available to training events such as unit training at the National Training Center. Those forces were more aware of different options and could make educated decisions regarding which one they employed. This training helped the users and commanders develop trust that these less familiar systems would advance their larger mission.

This kind of training also safeguarded those forces from another problem seen in Iraq and Afghanistan: not understanding a new and unfamiliar system that was available and so using it in a suboptimal way, different from its intended application. At best, this led to valuable technology being used in ways that were not productive. The lack of understanding could also lead to an increased risk of poor decisions being made, missed opportunities, and inadvertent engagements.

For autonomous systems, this kind of training and familiarization process at the operator and operational commander level would also promote trust and a more informed use of these kinds of capabilities. At the same time, the training requirements are likely to be more robust, since systems employing autonomy, and AI in particular, will have the ability to adapt and learn, depending on the operational environment, the nature of the threat, and the mission. Thus it likely will be necessary for operators and operational commanders to work with these systems more extensively and over a wider range of scenarios for such systems to become relatively predictable and acquire an appropriate degree of trust. It has also been noted that humans tend to be more forgiving of breeches of trust committed by other humans than they are of machines doing the same.[68] This suggests that it may not be sufficient for military systems employing autonomy and AI to reach equivalence with human performance but, rather, that they will need to be able to demonstrate that they exceed that performance before they are accepted and trusted in practice.

U.S. senior leaders

Senior military and government leaders also influence the nature of military operations, and use of specific technologies in war through policy decisions. These policies can influence levels of oversight (DODD 3000.09 requiring a senior level

[68] Ilachinski, *AI, Robots, and Swarms.*

review of some types of autonomous systems), kinds of allowable technology (cluster munitions directive setting requirements on characteristics needed for such weapons to be used), and policy parameters in certain types of operations—for example, the 2013 Presidential Policy Guidance (PPG) outlining an approval and oversight process for some counterterrorism operations. These policies help ensure that military activities are consistent with U.S. principles, values, and interests. Currently, the U.S. military operates under DOD Directive 3000.09, which governs the approval process for the development and fielding of systems using lethal autonomy. This Directive is not a ban on such systems but, rather, sets conditions for their development and approval. At the time of this report, there has been no system that has met the conditions where such a review would be required. As such systems are developed and fielded, it is possible that additional policy could be developed that governs their operational use, in addition to legal considerations. For example, policy could address questions such as whether unmanned autonomous systems will be permitted to use lethal force against personnel or manned platforms in self-defense. These policy-level determinations tend to reflect the level of trust held for the reliability of these systems.

Senior leaders in the military and government will be influenced by negative incidents involving autonomous systems, if they have occurred. This underscores the importance of measures such as those detailed in the previous section, "Reducing Risk in Lethal Autonomy." In the absence of such incidents, leaders likely will rely less on personal experience with such systems—since such experience may be rare, especially in their first years of fielding—and more on processes designed to demonstrate that such systems meet key requirements, such as the Test and Evaluation (T&E) process. However, the current T&E process is unsuited for factoring in the particular challenges of autonomous systems, especially those that can change and adapt over time. These systems will not be predictable from a deterministic sense, and so the traditional T&E paradigm will fail to answer the fundamental question of whether an autonomous system is capable of meeting its requirements for performance, while also keeping risks (e.g., inadvertent engagements) to a minimum.

One possibility for tailoring the T&E process for autonomy is to make T&E events iterative, where development efforts have discrete T&E elements at key milestones. This provides a larger body of evidence regarding the reliability of systems, as well as an opportunity to address key concerns that surface during earlier tests. This iterative process is not without precedent: for example, the Navy has employed an iterative approach to system testing through its Distributed Engineering Plant (DEP) process, intended to identify interoperability issues that are not necessarily evident in system-level testing, but can result when systems are interacting with other systems. The DEP process allows early identification of issues that otherwise might not be identified until the system is fielded. Such a DEP approach to testing autonomous systems can also be used to expand the operational scenarios evaluated

in T&E events. Live exercises can also be used to reveal system performance issues outside of the normal T&E process. For example, joint exercises in the 1990s and early 2000s helped resolve interoperability issues and refine CONOPS that were then used in air defense and time-sensitive targeting operations in Iraq in 2003. Such an expanded process would be especially valuable to mitigate increased risk from rapid acquisition processes that are envisioned for some autonomous and AI capabilities.

Another component of trust involves cyber security—having confidence that military systems will not be tampered with through cyberattacks. This could include wresting control of systems or alternately degrading or altering them so that they are ineffective or unreliable. While all military systems potentially can be tampered with, autonomous systems could be particularly vulnerable if they are used without operator involvement.[69] Thus particular attention will need to be placed on hardening these systems from intrusion and tampering.

Trust at the policy level will also affect other related considerations, such as export policies and processes. The Second Offset had as a primary element of its strategy denial of key technologies to potential adversaries, and—though it will be more difficult, given the dominance of the commercial sector on technological developments – similar export restrictions should be an element of the Third Offset to safeguard the technological edge of the U.S. military.[70] Yet there is also a question of what systems to export to allies, as well as what systems to support with U.S. components. For example, an indigenously developed system for using lethal force against people with little to no safety measures, using a key U.S.-produced component, both endangers civilians and imperils the reputation of the U.S. if some mishap were to occur. The U.S. will require an export policy, supporting technical experts, and accompanying review process to address this dilemma: this could begin with an interagency equivalent of the military's senior review prescribed in DODD 3000.09.[71]

[69] Brian K. Hall, "Autonomous Weapons Systems Safety," *Joint Force Quarterly* 86/3 (2017).

[70] Perry, "Desert Storm and Deterrence."

[71] Note that the section, "Mitigating Risk in Lethal Autonomy," includes considerations from which the senior review mandated in DODD 3000.09 would benefit.

Allies: supporting U.S. and coalition operations

Historically, the U.S. military almost always operates within a larger coalition, and this is likely to continue: "[There] are compelling reasons that suggest the U.S. will continue to operate in a coalition environment in the majority of future operations."[72] The size and nature of that coalition will vary, but even for the most sensitive and critical operations, the U.S. has tended to partner with a few close coalition partners. For example, while the U.S. turned down many offers of assistance for the initial invasion of Afghanistan in 2001, the UK and Australia were involved from the first months of the campaign.[73]

Alliances and coalitions could be considered an element of an offset strategy against adversaries that are expected to largely go it alone in operations. Working within a coalition offers a number of benefits to U.S. military operations. One is providing a greater collective mass in terms of forces available compared to each nation's individual contribution. Even smaller partners, when combined, can make a significant contribution—a larger number of troops for ground operations or ships/aircraft for operations in other domains—which is especially valuable for an enduring operation.[74] Another important benefit is greater legitimacy regarding an operation, including the right to wage war. International law provides justification for individual nations to begin an armed conflict under certain conditions; however, in practice, such actions can gain legitimacy if they have a mandate by an international body such as the United Nations or alternatively if operations are

[72] Joint and Coalition Operational Analysis Division, *Enduring Lessons from the Past Decade of Operations,* Vol. 1 (Suffolk, VA: JCOA, June 15, 2012).

[73] Alexander Powell, Larry Lewis, Catherine Norman, and Jerry Meyerle, *Summary Report: U.S.-UK Integration in Helmand,* CNA Occasional Paper DOP-2015-U-011259-Final.pdf, February 2016.

[74] In October 2014, there were 45 troop-contributing nations within NATO's International Security Assistance Force (ISAF). While the U.S. contributed the preponderance of the total forces (~25,000 personnel), the other contributing nations provided about 10,000 additional forces. Though the U.S. had the capacity to field the total number, because of coalition contributions, it did not need to.

conducted by a group of nations acting together (i.e., a "coalition of the willing"). This legitimacy can be decisive with regard to whether an operation is conducted.[75]

But coalition operations also create challenges not present in a unilateral operation. These challenges have been described as friction points of coalitions. Analysis has identified friction points that reduce the benefits of operating together while also increasing the costs and risks to coalition forces. These include friction points *associated with institutional military forces*—such as differences in force generation, interoperability, military culture, and computer information systems—as well as *national policy* friction points such as differing ROEs, detainee policies, and other national caveats.[76] Collectively, these friction points complicate integration efforts and reduce unity of effort among coalition partners.[77]

This has implications for the U.S. use of autonomy and AI in coalition operations. For example, the effective use and oversight of autonomous systems could be hindered by interoperability issues and by national policies and caveats. In an example of the impact of coalition interoperability issues, in Operation Iraqi Freedom in 2003, due to UK implementation decisions a UK E-3D was unable to provide oversight of Patriot systems during its unintended shoot-down of a U.S. Navy F/A-18C. Similar interoperability issues could negatively impact the operation of autonomous systems, which could tend to be more vulnerable to such deficiencies.[78]

Similarly, national policies and caveats could limit the use of autonomy and AI, or have broader effects on coalition effectiveness. For example, different national policies for the use of autonomy and AI in decisions involving lethal force could limit intelligence provided to the U.S., when it could be used for targeting (similar to how the UK limited intelligence sharing to the U.S. in Afghanistan due to differences in detainee handling policies).[79] While many U.S. allies have not yet articulated a clear

[75] For example, Army Field Manual FM 3-16, *The Army in Multinational Operations* (May 2010), states: "Another reason the U.S. conducts such [multinational] operations is that rarely can one nation go it alone.… This blending of capabilities and political legitimacy makes certain operations possible that the U.S. could not or would not conduct unilaterally." This effect was also seen in the proposal for the use of force against the Syrian regime in summer 2013. When the U.S. did not have coalition partners such as the UK willing to join, the decision was made to forego that proposal.

[76] Powell et al., *Summary Report: U.S.-UK Integration in Helmand.*

[77] Churchill aptly described both the benefits and challenges of coalitions when he said near the end of World War II: "There is only one thing worse than fighting with allies, and that is fighting without them."

[78] This effect is elaborated on in the companion chapter, "Interoperability and Support to Autonomous Targeting."

[79] Powell, et al., *Summary Report: U.S.-UK Integration in Helmand.*

policy on autonomous weapon systems, already a key ally—the UK—has a significantly different position from that of the U.S., stating: "the UK does not possess armed autonomous aircraft systems and it has no intention to develop them. The UK government's policy is clear that the operation of UK weapons will always be under human control as an absolute guarantee of human oversight, authority, and accountability."[80] There are potentially many implications of this significant policy difference between the U.S. and the UK—an alliance often characterized by both sides as a special relationship.

The time to discover these coalition friction points is not during an operation. Discovering such friction points in the middle of an operation, without previous planning and mitigation steps in place, can result in the U.S. being unable to use its full set of capabilities or having to develop what can turn out to be less-then-optimal workarounds in the field. In order to fully leverage the dual deterrents of autonomy and our broad set of allies, coalition policy and interoperability friction points associated with the use of autonomy and AI should be identified early, with efforts made with our allies to resolve and/or articulate the many implications of these policy differences in advance.

International community: maintaining legal and normative freedom of action

Of course, the United States does not simply operate under its own auspices and that of its close allies. The larger international community has a significant role in shaping military operations—both the decisions to launch them and the conduct of those operations. For example, the UN Charter encapsulates key justifications for states waging armed conflict against other states, and UN resolutions can authorize the use of force in specific conflicts, in addition to national self-defense considerations. Similarly, the conduct of combatants in armed conflict is governed by international law, as well as international conventions and treaties. This includes treaties and conventions on certain types of weapons. The use of weapons can be controlled in different ways, such as

- **Outright bans.** Some weapons are considered so inhumane that their possession or use is banned entirely. An example of this is the Chemical Weapons Convention (CWC), which comprehensively prohibits chemical

[80] Joint Doctrine Publication (JDP) 0-30.2, *Unmanned Aircraft Systems,* UK Ministry of Defence, dated August 2017.

weapons, including use, development, production, storage, and transfer. The CWC was approved in 1992, and entered into force in 1997.[81]

- **Limits on usage.** Other weapons are not considered inherently inhumane or unlawful, but certain uses are considered to be so. An example of this is the Convention on Certain Conventional Weapons (CCW) Protocol II, Mines, Booby Traps and Other Devices.[82] This protocol limits the use of land mines, remotely delivered mines, or booby traps in order to avoid unnecessary suffering to soldiers or civilian casualties. The original protocol was approved in 1980, and entered into force in 1983. A strengthened, amended protocol was approved in 1996, and entered into force in 1998.

- **Banning specific effects on humans.** Weapon usage can also be curtailed to limit specific effects against humans. An example of this is the CCW Protocol IV, Blinding Laser Weapons. This convention prohibits lasers as weapons intended to cause blindness to humans. It was approved in 1995, and entered into force in 1998.[83] This convention was also said to be the first pre-emptive ban of a weapon that had not yet been fielded.

- **Consultations.** International dialogue with other States and groups such as ICRC can discuss the legal and humanitarian effects of weapons that are legally permissible, but may be a concern in certain operations or contexts. These do not necessarily result in formal treaties or agreements but can shape U.S. policy and practice.

This is germane to autonomous weapons as the CCW has held a series of meetings on lethal autonomous weapon systems. To date, those meetings have been general consultations among member states to discuss legal, ethical, and operational considerations of these future weapon systems. To date the U.S. and the majority of member states favor continuing consultations without the expectation of an additional Protocol banning these weapons, seeing this as premature. However, more than a dozen states have indicated that they favor a preemptive ban. The United States continues to be involved in these international discussions, emphasizing that

[81] The Chemical Weapons Convention can be found in its entirety at https://www.opcw.org/chemical-weapons-convention/.

[82] The CCW is shorthand for the United Nations Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects. The CCW is a multilateral convention under the United Nations. See United Nations Office for Disarmament Affairs (UNODA), https://www.un.org/disarmament/geneva/ccw/amended-protocol-ii/.

[83] CCW, https://www.un.org/disarmament/ccwc_p4/.

from their perspective, any U.S. military use of lethal autonomous weapon systems will comply with international law, as well as U.S. values and principles.

Because these conventions and treaties can limit the U.S. both in equipping for and its conduct of war, the U.S. has interests in helping shape international law and associated norms associated with armed conflict. Sometimes these deliberations can turn out poorly for the U.S. For example, the recent cluster munitions ban reflected a direction that the U.S. was unwilling to take in light of its national interests, despite it having strong interest in setting guidelines that would better protect civilians.[84] As a result, the U.S. is not a signatory to the cluster munitions ban, though it developed its own cluster munitions policy that restricts the types of munitions it can procure and use. The U.S. receives criticism for not being a signatory, and not being part of a ban on cluster munitions means that it is easier for other states to go their own way with regard to cluster munitions use, without the policy commitments that the U.S. has made. And the cluster munitions ban itself is less than optimal, banning a wide variety of weapons including the CBU-105 sensor fused cluster munition that has extensive safeguards and, in some settings, can be preferable to a conventional bomb for the purposes of civilian protection.

A more positive example in the U.S. shaping international law and norms has been the use of armed drones. U.S. counterterrorism operations featuring targeted killing by armed drones was the subject of much criticism, and there were calls for developing international restrictions on their use.[85] However, the U.S. took a proactive approach, developing a policy framework for these operations (the 2013 Presidential Policy Guidance for counterterrorism operations outside of declared areas of conflict) that mandated interagency review and oversight while introducing strict standards for target identification and avoiding civilian casualties.[86] This was accompanied by initiatives to increase transparency regarding the associated process, the overall justification for the use of force in these operations, and the level of care taken to exceed the requirements of international humanitarian law. As the U.S. proactively took on these measures, both international and domestic

[84] This refers to the Convention on Cluster Munitions, which "prohibits all use, stockpiling, production, and transfer of cluster munitions." United Nations Office for Disarmament Affairs (UNODA), https://www.un.org/disarmament/ccm/.

[85] Larry Lewis and Diane Vavrichek, *Rethinking the Drone War: National Security, Legitimacy, and Civilian Casualties in U.S. Counterterrorism Operations,* Quantico, VA: Marine Corps University Press, 2017.

[86] Procedures for Approving Direct Action against Terrorist Targets Located Outside the United States and Areas of Active Hostilities, May 22 2013, https://www.justice.gov/oip/foia-library/procedures_for_approving_direct_action_against_terrorist_targets/download.

criticism decreased, and the international community's interest in normative restrictions on armed drone usage declined.

The example of armed drones illustrates how responsible behavior with a weapon type, especially when accompanied by transparency measures intended to reinforce and model this behavior, can help preserve operational freedom of action. These ingredients can be useful in the U.S. making the responsible case for freedom of action for lethal autonomous weapon systems as well. Though these weapons are not currently used operationally, U.S. policies and specific safeguards that will be put in place to ensure their responsible and careful use could help to counter the calls for an international ban. This is critical for the U.S. goal of having these weapons as a credible deterrent, and this deterrent effect will be less credible if their use is banned internationally.

Civil society and media: important influencers

Civil society groups and media reporting can have a significant impact on the conduct of armed conflict. These groups can also have significant influence on international proceedings such as the CCW, serving in their valuable watchdog role on the conduct of war. While their perspectives—and for civil society groups, even their legal framework—may be different than that of the U.S., they can have useful perspectives overall, as well as unique information regarding specific allegations that the U.S. can consider.

This role is clearly seen for the case of lethal autonomy. The NGO Campaign to Stop Killer Robots is a prominent voice in the call to preemptively ban these weapons. This and other advocacy organizations (for example, Human Rights Watch) have put significant pressure on the CCW to continue serious discussions on lethal autonomy, including the formation of a Group of Government Experts (GGE). The GGE was approved by the CCW in December 2016 at the Fifth Review Conference, and they are scheduled to meet for the first time in November 2017. Similarly, many media reports cover the controversy over lethal autonomy, as well as efforts like the Campaign to Stop Killer Robots and groups of scientists stating their concerns over the militarization of artificial intelligence. While they may have a different perspective, it is still useful to engage with these organizations and communicate a shared concern for the safety of these systems and a shared commitment to uphold international law and promote civilian protection. These continued dialogues can both improve the ability of the U.S. to safeguard against potential risks and also share the specific measures the U.S. plans to use to mitigate risk (and the rationales for them). These measures, such as a policy on lethal autonomy and legal weapons

reviews, could potentially be standard practices that other states could adopt in order to promote responsible use of these emerging technologies.

In addition to influencing international deliberations, these groups can also influence U.S. government leaders. For example, regarding U.S. assistance to the Saudi coalition's operations in Yemen, groups like Human Rights Watch and Amnesty International had a robust outreach effort to share on-the-ground evidence their teams had developed, as well as concerns about violations of IHL by both the Saudi coalition and, by extension, the U.S. government because of its support. While these groups provided valuable on-the-ground information, their legal and operational conclusions differed markedly from that of the U.S. government in DOD and at State. However, congressional members heard only one side of the argument from these groups and from media reporting of their findings. Consequently, it could be valuable for the U.S. government to not neglect its own Congress as an audience when making arguments for the legality and benefits of lethal autonomous systems.

Legitimacy: a lesson from the second offset

The Second Offset involved precision strike, ISR, and the use of stealth to combat the Soviet Union's numerical advantage by increasing the targeting effectiveness of individual strikes. While the goal of the Second Offset was precision and increased effectiveness with fewer munitions expended, the second-order effects of this capability was the ability to conduct operations more surgically and humanely, with greatly reduced collateral damage.[87] This capability to conduct operations with precision and with reduced cost to the civilian population, as exhibited in Operation Desert Storm and subsequent operations in Iraq, Afghanistan, Libya, and elsewhere, gave the U.S. freedom of action in order to address what it considered imminent threats, such as those targeted in its counterterrorism operations outside of declared areas of conflict. At the same time, this new capability—and continued U.S. commitment to using this capability to protect civilians—blunted criticisms from others and indeed has served as a model for other states using force, promoting legitimacy and U.S. national interests.[88]

The elements of the Third Offset can potentially hold the same benefits as technologies used in the Second Offset: effectiveness, precision, improved

[87] Perry, "Desert Storm and Deterrence."

[88] In recognition of its importance, U.S. military doctrine added legitimacy to its list of "principles of Joint operations." This list constitutes a set of best practices that should be followed for any conflict. Joint Staff, Joint Publication 3-0, *Joint Operations,* August 11, 2011.

discrimination, and reduced collateral damage. The potential technological benefits of autonomy and AI include more than just the ability to more effectively engage a target. They also hold promise for additional measures for protecting civilians. For example, an airborne autonomous strike platform could be more maneuverable and/or have a longer flight time, giving that platform more options for using force from different vantage points and deciding the optimal time and place, using tactical patience as needed. These systems could also be equipped with new forms of munitions designed to be particularly effective with very limited collateral damage. AI capabilities such as voice recognition and image recognition could also be harnessed to improve discrimination of combatants and potentially reduce the existing problem of misidentification in U.S. operations.

If the U.S. military includes these same goals in policy, in system requirements, and in concept development, then the Third Offset can help the U.S. to enjoy the same benefits of greater legitimacy and enhanced freedom of action. In addition, these goals of greater precision and civilian protection are consonant with many other parties, even groups that explicitly oppose the use of lethal autonomy. While improved military effectiveness from the Third Offset is an imperative for the U.S. military, showing how autonomy can also contribute to larger humanitarian goals can be the most powerful argument against a ban to other audiences and may promote greater understanding and even support of U.S. goals and actions.

To that end, the U.S. can incorporate this argument into its policy and practice by articulating this aim in policy, setting appropriate system requirements, and including civilian protection and discrimination in experimentation venues in order to promote development of CONOPS, tactics, and doctrine that support this goal. The U.S. can then communicate this commitment to allies, international audiences, and important influencers such as civil society groups and the media.

Recommendations

Familiarization training. Provide extensive familiarization training for operators and operational commanders regarding systems with autonomy and artificial intelligence, preferably over a wide range of scenarios and missions.

New approach to Test and Evaluation. Develop a new approach to Test and Evaluation processes for systems employing autonomy and AI to ensure reliability and confidence in non-deterministic systems. This new approach could feature

- An iterative approach with nested development and testing
- Leveraging simulation and distributed testing capabilities similar to the Navy's Distributed Engineering Plant

- Using live exercises to give additional opportunities to observe behavior and identify concerns.

Export policy for autonomy. The U.S. government should develop a U.S. export policy and accompanying review process to address the risks of U.S. technology being used in lethal autonomy by others. That could begin with an interagency equivalent of the military's senior review prescribed in DODD 3000.09.

Identify and address coalition friction points. Work with allies to resolve policy and interoperability issues associated with the operational use of autonomy and AI. Start with key allies such as the UK, Australia, and Canada.

Substantive engagements: with Congress, in international venues, and with civil society groups. Continue meaningful involvement with Congress and in the CCW and other international forums regarding autonomy and AI in military operations. Also continue engagements with concerned civil society groups. This involvement should stress constructive arguments including showing how autonomy and artificial intelligence in military operations can contribute to humanitarian goals.

Learn from the Second Offset. The U.S. military should learn from the success of the Second Offset and include both precision and promoting humanitarian goals such as sparing civilians in war in its implementation of and communications regarding the Third Offset. That includes articulating the aim of civilian protection in policy, setting appropriate system requirements, and including civilian protection and discrimination in experimentation venues in order to promote development of CONOPS, tactics, and doctrine that support this goal.

Conclusions

The U.S. military is relying on the incorporation of artificial intelligence and the AI-enabled capability of autonomy as the initial underpinnings of its new national military strategy. These new technologies hold much promise and can potentially deliver important capabilities that can deter high-end conflict from near-peer competitors. However, success in this endeavor is not assured.

The current environment, where the U.S. military edge is contested and, at the same time, the commercial sector leads the research and development of key technology, means that the U.S. is on new and unfamiliar ground. Instead of just relying on its established military-industrial complex for solutions, it will need to compete in a race in time where the U.S. must be able to identify new capabilities in an agile way and then integrate them into military systems before other peer competitors do (as well as nonstate actors). While DOD has created a number of initiatives to streamline commercial industry proposals to meet military requirements, this falls short of what DOD will need to do to acquire cutting-edge capabilities in order to maintain a military edge. Overall, it will need to adopt a new fast-follower posture with respect to commercial technological developments. This includes tracking the militarization of this technology by other states and by non-state actors and refining its own approach accordingly.

One of the lessons of the Second Offset is that networked systems offer tremendous advantages, but there are interoperability challenges that come with that interdependence and networking approach. These interoperability challenges limit overall effectiveness, reducing the effective range that weapons can be used, as well as contributing to friendly fire incidents. Due to their intermittent connectivity and their reliance on certain information for their missions, it is likely that autonomous weapon systems will be even more susceptible to interoperability challenges. These challenges can be overcome, but they require attention to the design, testing, and early fielding of these systems.

Part of this effort is mandated in policy—DODD 3000.09—which calls for efforts to avoid unintended engagements by lethal autonomous systems. This policy goal can be promoted by having systems designed and operated in ways that learn lessons from past incidents. The U.S. military has done much work in reducing friendly fire and civilian casualties in its operations, and many of these principles can be used to make lethal autonomy safer. The mandated senior-level review for fully autonomous

systems can include validating that these elements have been considered in their design and projected use. Another critical aspect for systems employing autonomy and AI is to adapt current Test and Evaluation practices, which rely on repetitive tests to determine reliability, addressing systems that are non-determinative and can learn and adapt.

One of the essential elements of the Third Offset strategy is an exploration of alternatives and discovering what options give the most benefit. Experimenting with technology and tactics was also essential to the success of the Second Offset. While experimentation can take many forms and be done at different levels of rigor, one danger of experiments is that they can be evaluated subjectively. One lesson learned from exercises and even operations is that things may seem to work from an operator perspective, and that is judged as success; however, when the data are analyzed, that operator's perception may not match the facts. Using data collection and analysis to supplement and confirm operator and observer impressions can help experiments to come up with accurate conclusions. They also give additional opportunity to determine the root cause of deficiencies and develop better solutions to those deficiencies. Combining data and analysis with experimentation can help the U.S. to have an edge in the Third Offset's competition of time.

The U.S. military is pursuing autonomous systems because they can be more effective in specific operational scenarios, but there are many who have raised concerns about such systems—especially when using lethal force. A lesson from the Second Offset is that technology and precision can help military systems to be more effective and simultaneously cause fewer civilian casualties, demonstrating that there are decided humanitarian benefits to these types of systems—in addition to the strategic benefits of sustaining U.S. operational legitimacy and preserving operational freedom of action. The latter benefits do not depend on the U.S. military alone, however: Other audiences also matter, including senior U.S. government and military leaders, key allies, international forums, NGOs, and the media.

A similar focus and narrative with the Third Offset could have a similar effect. If the U.S. military actively includes the goals of effectiveness, precision, improved discrimination, and attenuated collateral damage in policy, in system requirements, and in concept development, the Third Offset can help the U.S. enjoy the same benefits of greater legitimacy and enhanced freedom of action—goals that are consonant with those of many other groups, even groups that explicitly oppose the use of lethal autonomy. While improved military effectiveness from the Third Offset is an imperative for the U.S. military, showing how autonomy can also contribute to larger humanitarian goals can be the most powerful argument against a ban on autonomous weapon systems in general, and may promote greater understanding and even support of U.S. goals and actions to try to deter conflict situations across the globe.

Though not explored in depth in this report, there are a number of other issues with regard to the Third Offset implementation that are important to consider. Perhaps the most significant is the requirement for basic research and framework development for AI and autonomy. Though DOD is moving ahead with experimentation and even design and fielding of systems with various degrees of autonomy, there are many underlying concepts and issues of importance that have yet to be developed. This means that there may be fertile areas that will go unexplored. Just like basic research in science led to innovative capabilities like the laser, the integrated circuit, and GPS—all extensively used in military applications—foundational work in AI and autonomy should be expected to have similarly strong and unexpected benefits. This should also be an area of focus for DOD in the near future.

Recommendations

Many advances, some unforeseeable, are expected in the coming decades because of technological advances involving autonomy and AI. At the same time, there are actions the U.S. can take now to best prepare for these advancements and leverage them effectively. This report details four deliberate efforts needed in the near term to overcome key challenges in leveraging autonomy and AI in the Third Offset. Those efforts are:

- Becoming a fast follower to rapidly develop capabilities leveraging key technologies
- Prioritizing interoperability of autonomous systems to improve their effectiveness
- Taking specific actions to help autonomous weapon systems avoid mishaps such as friendly fire and civilian casualties
- Promoting freedom of action for the use of autonomy and AI in operations with multiple audiences

Recommended actions for each of these imperatives are discussed in turn.

Aim to be an effective fast follower of autonomous and artificial intelligence technologies. This includes the following actions:

- **Build DOD technical expertise.** Cultivate technical expertise on autonomy and AI in the military services capable of identifying specific technical requirements needed for achieving military capabilities. This includes addressing organizational disincentives for maintaining personnel with high levels of technical expertise.
- **Prioritize military R&D resources, leveraging a fast-follower approach.** Instead of trying to cover all aspects of autonomy and AI, prioritize R&D resources to areas of the highest importance, or to areas not receiving attention in the commercial sector.
- **Monitor and integrate specific commercial developments.** DOD technical expertise should track targeted autonomy and AI developments in the commercial sector, looking for ways to rapidly integrate those developments

into military systems. These needs should also be advertised to industry to encourage their research and development in these areas

- **Track developments by others.** Track technological developments towards militarization of autonomy and artificial intelligence by key states and nonstate actors, leveraging them for evaluation of U.S. operational plans, needed U.S. capabilities, and possible ways the U.S. can learn from these other efforts.

- **Introduce a learning loop.** Conduct in-stride learning efforts for existing DOD innovation initiatives (e.g., Project Maven) in order to make efforts meeting urgent operational needs through autonomy and AI more effective.

Prioritize interoperability of autonomous systems. This includes:

- **Programmatic focus on interoperability:** program offices give close attention to interoperability for autonomous systems, especially for those using lethal force, given the greater vulnerability autonomous systems can have to interoperability challenges. These include

    - Determining specific information requirements for the use of lethal autonomy

    - Designing systems with communication capabilities to support these requirements

    - Adopting best practices for interoperability: pursuing common architectures, making standards for data link implementation, and enforcing their implementation for applicable Program Offices.

    - End-to-end interoperability testing, not simply interface format compliance tests.

- **Policy requirement for interoperability:** Make a requirement for observing interoperability best practices as part of the senior review of fully autonomous systems required in DODD 3000.09.

- **Reduce risk through live events:** Use regularly scheduled risk-reduction live events (such as exercises) throughout the development life-cycle of autonomous systems to reduce risk. This should include instrumented systems in operationally realistic environments in order to provide early warning of potential deficiencies and give opportunities to evaluate potential fixes.

- **Marry data and analysis with experimentation.** Include data collection and analysis during experimentation events in order to supplement and confirm

operator and observer impressions, and accelerate the process for improving capabilities overall.

Take specific measures to help lethal autonomous systems avoid inadvertent engagements, including:

- **Monitor for misidentifications.** Autonomous systems should give careful attention to the possibility of misidentification, including cross-checks of different kinds of identifying information and flagging potential conflicts or inconsistencies—for example, identifying that an entity has kinematics that are inconsistent with a suspected platform or target type.

- **Include robust IFF measures.** Sensors for autonomous systems should ensure compatibility with appropriate anti–friendly fire measures.

    - For example, an autonomous system that is able to engage air targets could include Mode 5 or Link 16 PPLI. For ground targets, the autonomous system could include Blue Force Tracker (BFT) reception or sensors able to detect infrared (IR) signatures (strobes or panels).

    - It should also be acknowledged that such systems have failed in the past as a single-source safety measure. Multiple measures are preferred when feasible; where they are not, a heightened risk of friendly fire should be understood.

    - This consideration should also extend to humanitarian applications—for example, the Geneva Conventions call for hospitals to display red crosses/crescents to indicate their protected status; autonomous systems operating in areas where hospitals could be present should have the ability to distinguish such markings.

- **Leverage available information.** Autonomous does not necessarily mean isolated. In light of mission requirements, autonomous systems should be provided with information and intelligence when possible to ensure current situational awareness and inform optimal engagement decisions. This should also include provision of current ROE and other guidance for the use of force to ensure engagements are consistent with commander's intent and applicable law.

- **Consider civilian casualties.** Autonomous systems should give careful consideration and make every precaution to avoid civilian casualties, consistent with measures U.S. forces have put in place for recent operations. These measures include

  - Compliance with IHL. This is a matter of extensive training for U.S. forces; autonomous systems must also be sure to comply with legal requirements for the use of force in armed conflict.
  - Not assuming that no civilians observed means no civilians present.
  - Taking additional measures to screen for collateral damage, such as pattern of life determinations and zooming out the field of view to screen for civilians
  - Exercising tactical patience when possible, and considering tactical alternatives

- **Develop DODD 3000.09 senior review criteria.** These considerations should be made part of the required senior-level review for development and fielding of autonomous systems per DODD 3000.09.

Take steps to be able to employ autonomy and AI in operations if necessary to deter and defend itself against critical threats:

- **Examine other risks of lethal autonomy.** This report examines the risk of inadvertent engagements by lethal autonomous weapon systems. A further study should examine a number of other potential risks presented by lethal autonomy that are humanitarian, ethical, and strategic in nature.
- **Familiarization training.** Provide extensive familiarization training for operators and operational commanders regarding systems with autonomy and artificial intelligence, preferably over a wide range of scenarios and missions.
- **New approach to Test and Evaluation.** Develop a new approach to Test and Evaluation processes for systems employing autonomy and AI to ensure reliability and confidence in non-deterministic systems. This new approach could feature
  - An iterative approach with nested development and testing
  - Leveraging simulation and distributed testing capabilities similar to the Navy's Distributed Engineering Plant
  - Using live exercises to give additional opportunities to observe behavior and identify concerns.
- **Export policy for autonomy.** The U.S. government should develop a U.S. export policy and accompanying review process to address the risks of U.S. technology being used in lethal autonomy by others. That could begin with

an interagency equivalent of the military's senior review prescribed in DODD 3000.09.

- **Identify and address coalition friction points.** Work with allies to resolve policy and interoperability issues associated with the operational use of autonomy and AI. Start with key allies such as the UK, Australia, and Canada.

- **Substantive engagements: with Congress, in international venues, and with civil society groups.** Continue meaningful involvement with Congress and in the CCW and other international forums regarding autonomy and AI in military operations. Also continue engagements with concerned civil society groups. This involvement should stress constructive arguments including showing how autonomy and artificial intelligence in military operations can contribute to humanitarian goals.

- **Learn from the Second Offset.** The U.S. military should learn from the success of the Second Offset and include both precision and promoting humanitarian goals such as sparing civilians in war in its implementation of and communications regarding the Third Offset. That includes articulating the aim of civilian protection in policy, setting appropriate system requirements, and including civilian protection and discrimination in experimentation venues in order to promote development of CONOPS, tactics, and doctrine that support this goal.

References

Andersen, Erika. May 31, 2013. "21 Quotes from Henry Ford on Business, Leadership, and Life." Forbes Magazine. https://www.forbes.com/sites/erikaandersen/2013/05/31/21-quotes - from- enry-ford-on-business-leadership-and-life/.

Anno, Stephen, and William E. Einspahr, 1988. "The Grenada Invasion." In *Command and Control Lessons Learned: Iranian Rescue, Falklands Conflict, Grenada Invasion, Libya Raid.* Air War College Research Report AU-AWC-88-043. Maxwell Air Force Base, Ala.: Air University Press. Reprinted as an extract from the original report by the U.S. Naval War College Operations Department, NWC 2082. http://www.fas.org/man/dod-101/ops/urgent_fury.htm.

Barrett, Carla. May 15, 2014. PowerPoint presentation. "Interoperability in DOD: Why is it so hard to attain?"

Blank, Steve. October 5, 2010. "You're Better Off Being a Fast Follower than an Originator." Business Insider. http://www.businessinsider.com/youre-better-off-being-a-fast- follower-than-an-originator-2010-10.

Boot, Max. July 25, 2003. "The New American Way of War." *New York Times.* http://www.nytimes.com/cfr/international/20030724faessayv82n4_boot.html?pagewanted=print&position.

Borsuk, Dr. Gerald M. April 13, 2016. Presentation at the National Defense Industrial Association Science and Engineering Technology Conference, Tampa, FL.

Chemical Weapons Convention. https://www.opcw.org/chemical-weapons-convention/.

Convention on Cluster Munitions, United Nations Office for Disarmament Affairs. https://www.un.org/disarmament/ccm/.

Defense Science Board. June 2016 *Report of the Defense Science Board Summer Study on Autonomy.* Washington, DC: Office of the Secretary of Defense. https://www.hsdl.org/?view&did=794641.

Defense Science Board. July 2012. *The Role of Autonomy in DOD Systems.* Washington, DC: Office of the Secretary of Defense. https://fas.org/irp/agency/dod/dsb/autonomy.pdf.

Department of Defense Research and Engineering. February 2015. *Technical Assessment: Autonomy,* Washington, DC: Office of Technical Intelligence, Office of the Assistant Secretary for Research and Engineering. http://www. Defense innovationmarketplace.mil/resources/OTI_TechnicalAssessment-AutonomyPublicRelease_vF.pdf.

Deputy Secretary of Defense. April 26, 2017. Memorandum: "Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)."

DOD Directive 3000.09. November 21, 2012. *Autonomy in Weapons Systems.*

Encyclopedia Britannica, s.v. "artificial intelligence," https://www.britannica.com/technology/artificial-intelligence.

Freedberg Jr., Sydney J. October 28, 2016. "Carter, Roper Unveil Army's New Ship-Killer Missile: ATACMS Upgrade." Breaking Defense. http://breakingdefense.com/2016/10/army-atacms-missile-will-kill-ships-secdef-carter/.

Freedberg Jr., Sydney J. November 9, 2015. "Centaur Army: Bob Work, Robotics, and the Third Offset Strategy." Breaking Defense. http://breakingdefense.com/2015/11/centaur-army-bob-work-robotics-the-third-offset-strategy/.

Greenwalt, William C. October 15, 2014. "Scraping off the barnacles of the defense acquisition system." AEI. http://www.aei.org/publication/scraping-barnacles-defense-acquisition-system/print/.

Grier, Peter. June 2016. "The First Offset." *Air Force Magazine.*

Ilachinski, Andrew. January 2016. *AI, Robots, and Swarms: Issues, Questions, and Recommended Studies.* CNA Research Memorandum DRM-2017-U-014796-Final.

Hagel, Chuck. November 15, 2014. Keynote speech delivered at Reagan National Defense Forum, Ronald Reagan Presidential Library. https://www.defense.gov/News/Speeches/Speech-View/Article/606635/.

Hall, Brian K. 2017. "Autonomous Weapons Systems Safety." *Joint Force Quarterly* 86/3.

Headquarters, Department of the Army. May 2010. *The Army in Multinational Operations.* Army Field Manual FM 3-16.

International Committee of the Red Cross. March 26–28, 2014. *Autonomous Weapon Systems: Technical, Military, Legal, and Humanitarian Aspects.* Geneva, Switzerland: ICRC. https://www.icrc.org/en/.../4221-002-autonomous-weapons-systems-full-report.pdf.

Jackson, Van. October 30, 2014. "Superiority at Any Price? Political Consequences of the First Offset Strategy." War on the Rocks. https://warontherocks.com/2014/10/superiority-at-any-price-political-consequences-of-the-first-offset-strategy/.

Joint and Coalition Operational Analysis Division. June 15, 2012. *Enduring Lessons from the Past Decade of Operations,* Vol. 1. Suffolk, VA: JCOA.

Joint Staff. August 11, 2011. *Joint Operations.* Joint Publication 3-0.

Kaplan, Fred. December 19, 2016. "The Pentagon's Innovation Experiment." MIT Technology Review. https://www.technologyreview.com/s/603084/the-pentagons-innovation-experiment/.

Lamothe, Dan. July 19, 2017. "The Pentagon has tried to get Silicon Valley on its side for years. Now it's part of the air war against ISIS." *Washington Post.* https://www.washingtonpost.com/news/checkpoint/wp/2017/07/19/the-pentagon-has-tried-to-get-silicon-valley-on-its-side-for-years-now-its-part-of-the-air-war-against-isis/?utm_term=.c6f29404d2e8.

Lewis, Larry. 2008. "Improving Joint C2: Lessons from Iraq." Presentation at the SMI Network-Centric Warfare Conference.

Lewis, Larry. May 17, 2006. "Death by 1,000 Ant Bites." CNA briefing to Chief of Naval Operations.

Lewis, Larry. July 2004. *Operation Iraqi Freedom: Ground-to-Air Fratricide* (U). CNA Research Memorandum CRM D0008910.A4. Secret. (Portions cited in the present report are unclassified.)

Lewis, Larry, and Sarah Holewinski. 2013. "Changing of the Guard: Civilian Protection for an Evolving Military." *Prism* 4, no. 2.

Lewis, Larry, and Paul R. Syms. October 31, 2006. *UK and U.S. Friendly Fire in Recent Combat Operations.* TTCP Technical Report DOC–JSA–AG13–3–2006.

Lewis, Larry, and Diane Vavrichek. 2017. *Rethinking the Drone War: National Security, Legitimacy, and Civilian Casualties in U.S. Counterterrorism Operations.* Quantico, VA: Marine Corps University Press.

Lewis, Lawrence, Jay Smith, Timothy Roberts, Bruce Behrens, and Paul Symborski. December 2002. *Performance of the Integrated Air Defense System at JCIET 02: SIAP, Interoperability, and Operational Considerations.* CNA Research Memorandum D0007309.02-Final. Secret. (Portions cited in the present report are unclassified.)

Mehta, Aaron. December 5, 2016. "Work: Munitions, Strategic Capabilities Office Boosted in FY18 Budget Plan." Defense News. https://www.defensenews.com/digital-show-dailies/reagan-defense-forum/2016/12/05/work-munitions-strategic-capabilities-office-boosted-in-fy18-budget-plan/.

Miller, Scott Alan. October 17, 2016. "No One Ever Got Fired for Buying…". SMB IT Journal. http://www.smbitjournal.com/2016/10/no-one-ever-got-fired-for-buying/.

Mullins, Marsha. October 1, 2014. "Joint Force Digital Interoperability Remains Elusive." *Signal.* https://www.afcea.org/content/joint-force-digital-interoperability-remains-elusive.

Nelson, Julianne, Charles Porter, and Kory Fierstine. March 2017. *RPED: A New Rapid Prototyping Strategy in the Department of the Navy.* CNA Research Memorandum DRM-2017-U-014757-Final.

Pearson, David. May–June 2015. "The Fast Follower: Coming Up Behind Development Leaders." *Defense AT&L,* May–June 2015, https://www.dau.mil/library/defense-atl/DATLFiles/May-Jun2015/Pearson.pdf.

Pellerin, Cheryl. November 3, 2016. "DOD Strategic Capabilities Office is Near-Term Part of Third Offset." DOD News. https://www.defense.gov/News/Article/Article/995438/dod-strategic-capabilities-office-is-near-term-part-of-third-offset/.

Pellerin, Cheryl. October 31, 2016. "Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence." DOD News. https://www.defense.gov/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence.

Pellerin, Cheryl. February 24, 2015. "DOD Seeks Novel Ideas to Shape Its Technological Future." DOD News. https://www.defense.gov/News/Article/Article/604159/dod-seeks-novel-ideas-to-shape-its-technological-future/.

Perry, William. Fall 1991. "Desert Storm and Deterrence." *Foreign Affairs.* https://www.foreignaffairs.com/articles/iraq/1991-09-01/desert-storm-and-deterrence.

Powell, Alexander, Larry Lewis, Catherine Norman, and Jerry Meyerle. February 2016. *Summary Report: U.S.-UK Integration in Helmand.* CNA Occasional Paper DOP-2015-U-011259-Final.pdf.

Procedures for Approving Direct Action against Terrorist Targets Located Outside the United States and Areas of Active Hostilities. May 22 2013. https://www.justice.gov/oip/foia-library/procedures_for_approving_direct_action_against_terrorist_targets/download.

"Putin: Leader in Artificial Intelligence Will Rule the World." Associated Press. September 1, 2017.

Radvanyi, Richard A. 2000. "Operation Eagle Claw: Lessons Learned." Unpublished thesis. United States Marine Corps Command and Staff College.

Ratz, Leon. September 2013. *Organizing for Arms Control: The National Security Implications of the Loss of an Independent Arms Control Agency.* Project on Managing the Atom Discussion Paper #2013-06. Belfer Center for Science and International Affairs/JFK School of Government.

Richardson, ADM John. January 17, 2017. Interview. Defense One. http://www.defenseone.com/ideas/2017/01/watch-d-brief-live-interview-chief-naval-operations-adm-john-richardson/134893/.

Sessions, Sterling D., and Carl R. Jones. July 1993. *Interoperability: A Desert Storm Case Study,* McNair Paper 18, Washington, DC: National Defense University/Institute for National Strategic Studies, http://www.dtic.mil/dtic/tr/fulltext/u2/a271674.pdf.

Stumborg, Michael. August 2016. *Finding the Off Ramp after a Decade of Rapid Acquisition.* CNA Research Memorandum DRM-2016-U-014007-Final.

Thielmann, Greg. 2006. "Intelligence in Preventative Military Strategy." In William W. Keller and Gordon R. Mitchell, eds. *Hitting First: Preventative Force in U.S. Security Strategy.* Pittsburg, PA: University of Pittsburg Press.

Tomeo, Robert. January 14, 2015. "Why the Cold War Offset Strategy Was All about Deterrence and Stealth." War on the Rocks. https://warontherocks.com/2015/01/why-the-cold-war-offset-strategy-was-all-about-deterrence-and-stealth/.

UK Ministry of Defence. August 2017. *Unmanned Aircraft Systems.* Joint Doctrine Publication 0-30.2.

United Nations Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects. United Nations Office for Disarmament Affairs. https://www.un.org/disarmament/ geneva/ccw/amended-protocol-ii/.

Unmanned Systems Integrated Roadmap, FY2013–2038. 2013. Washington, DC: Office of the Secretary of Defense. https://www.defense.gov/Portals/1/Documents/pubs/DOD-USRM-2013.pdf.

Wallace, Mark. April 3, 2017. "How Veterans Turned Entrepreneurs Are Disrupting The Pentagon's Weapons Program." Fast Company. https://www.fastcompany.com/40401930/how-military-veterans-turned-entrepreneurs-are-disrupting-the-pentagons-weapons-program.

Whaley, Greg, and Dana Stewart. April 2014. "Path from Urgent Operational Need to Program of Effort." *Defense ARJ* 21, no. 2. http://dau.dodlive.mil/2014/04/01/path-from-urgent-operational-need-to-program-of-record-2/#more-409.

Wikipedia. "Offset Strategy." Last modified January 21, 2017. Accessed April 2, 2017. https://en.wikipedia.org/wiki/Offset_strategy.

This page intentionally left blank.

CNA

DRM-2017-U-016281-Final-2

CNA
ANALYSIS & SOLUTIONS

CNA is a not-for-profit research organization
that serves the public interest by providing
in-depth analysis and result-oriented solutions
to help government leaders choose
the best course of action
in setting policy and managing operations.

Nobody gets closer—
to the people, to the data, to the problem.

1942 CNA 2017
ANNIVERSARY
75 YEARS OF SERVICE
TO OUR NATION

www.cna.org • 703-824-2000

3003 Washington Boulevard, Arlington, VA 22201